ARBOREAL GALOIS REPRESENTATIONS

A DISSERTATION SUBMITTED TO THE GRADUATE DIVISION OF THE UNIVERSITY OF HAWAIʻI AT MĀNOA IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

IN

MATHEMATICS

AUGUST 2018

By

TJ Combs

Dissertation Committee:

Michelle Manes, Chairperson
Pavel Guerzhoy
Ruth Haas
Robert Harron
Asaf Hadari
Linda Furuto

ACKNOWLEDGMENTS

I'd like to thank my advisor Michelle Manes for her guidance during my time here in the PhD program. She has been there for not only when I had questions about Mathematics, but also about my life and the path that I would like to follow. Michelle has been incredibly supportive with my transition into working full time during my final semesters in graduate school. Because I was working everyday during the week, she took the time on Saturdays to meet up with me at Starbucks to help me with my thesis. I'm very grateful for everything she has done for me.

Thank you Rob Harron for the time you have spent in graduate lounge answering my many questions. The conversations we've had have been transformed into ideas that occur in this thesis.

I'd like to thank the people who have decided to create the undergraduate and graduate lounge. Not only were these lounges a great place work on Mathematics, but they were also a great place to make friends and enjoy the company of really fun people.

I'd like to thank all the students, faculty, and staff of the Mathematics department for making me feel like the Mathematics department is like my home. My time in this department was truly an enjoyable experience.

I thank my parents for supporting me with all of my goals and for the constant push to become better.

And last but not least, I thank my wonderful partner Emilio for the unconditional support that he has given me all of these years. I would not have made it if were not for all the sacrifices that you have made.

ABSTRACT

We provide some general tools that can be used for polynomials in any degree to show $G_\infty = \mathrm{Aut}(T_\infty)$. We introduce the idea of Newton irreducibility to help push us closer to a proof to Odoni's conjecture for monic integer polynomials when $d = 4$. We also show that current techniques used in the literature will not work in proving Odoni's conjecture for monic quartic polynomials. Finally, we look at how certain behaviors of the critical points of a polynomial $f(x) \in K[x]$ force G_∞ to have infinite index in $\mathrm{Aut}(T_\infty)$.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1
INTRODUCTION

Let K be a number field and let $f(x) \in K[x]$ be a polynomial of degree $d \geq 2$. Our general setup follows the work of Jones [8] on arboreal Galois representations. Let $f^n(x)$ denote the n-fold iterate of $f(x)$ and let K_n be the splitting field of $f^n(x)$ over K. Notice that if α is a root of $f^{n+1}(x)$, then $f(\alpha)$ is a root of $f^n(x)$, therefore the fields K_n form a tower of fields Galois over K. Define

$$K_\infty = \bigcup_{n=0}^{\infty} K_n.$$

The field K_∞ is Galois over K since it is the splitting field of the infinite family of polynomials

$$f(x), f^2(x), f^3(x), f^4(x), \ldots.$$

Define $G_n = \mathrm{Gal}(K_n/K)$ and $G_\infty = \mathrm{Gal}(K_\infty/K)$. The main question of this paper is as follows:

Question 1. *When is G_∞ as large as possible?*

Since the K_n form a tower of fields, we get that $G_\infty \cong \varprojlim G_n$ via the isomorphism $G_\infty \to \varprojlim G_n$ defined by

$$\sigma \mapsto \left(\sigma\big|_{K_0}, \sigma\big|_{K_1}, \sigma\big|_{K_2}, \ldots\right).$$

The description of G_∞ above is quite abstract and does not give us much in our objective of answering our question. We turn to group actions to give us a better idea of the structure of G_∞. Let T_n be the tree with root 0 whose collection of vertices is

$$V_n = \bigsqcup_{k=0}^{n} f^{-k}(0).$$

We draw an edge between $\alpha \in f^{-k}(0)$ and $\beta \in f^{-(k-1)}(0)$ if $f(\alpha) = \beta$. The tree T_n is a regular d-ary tree for every $n \in \mathbb{N}$ provided that the forward orbit of the critical points of f avoid 0. For the rest of this paper, we will assume that our polynomials have this property. Let T_∞ be the inverse limit of T_n.

The group G_n acts faithfully on T_n by tree automorphisms. Since G_∞ is the inverse limit of G_n,

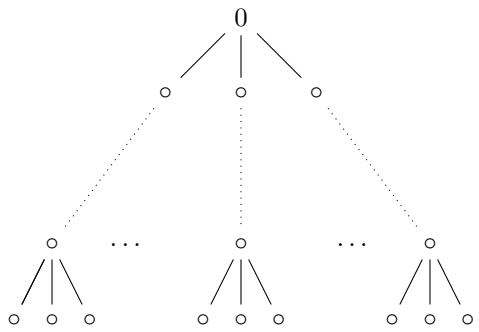

Figure 1.1: The preimage tree for a degree-3 polynomial.

we have an injective homomorphism

$$\rho : G_\infty \hookrightarrow \mathrm{Aut}(T_\infty),$$

called the *arboreal Galois representation of* $f(x)$. If the arboreal Galois representation of $f(x)$ is onto, we say that $f(x)$ has full arboreal Galois image. By abuse of notation, we will identify G_∞ with its isomorphic image under ρ and write $G_\infty = \mathrm{Aut}(T_\infty)$.

A major question in the study of arboreal Galois representations has been Odoni's conjecture. The following version of Odoni's conjecture is given by Jones in his survey article; it is Conjecture 2.2 in [8].

Conjecture 1 (Odoni's Conjecture)**.** *For each $d \geq 2$, there is a monic polynomial $f(x) \in \mathbb{Z}[x]$ of degree d with $G_\infty = \mathrm{Aut}(T_\infty)$.*

Odoni [14] provided a single quadratic polynomial with this property: $f(x) = x^2 - x + 1$. Stoll [17] gives several families of quadratic polynomials $f(x) \in \mathbb{Z}[x]$ such that $G_\infty = \mathrm{Aut}(T_\infty)$: $f(x) = x^2 + k$, where $-k$ is not a square, and one of the following holds:

- $k > 0$, $k \equiv 1 \pmod 4$,
- $k > 0$, $k \equiv 2 \pmod 4$, or
- $k < 0$, $k \equiv 0 \pmod 4$.

Though the conjecture dates to 1985, no example in degree greater than 2 was known until 2016 when Looper [13] described a family of trinomials in every prime degree $p \geq 5$ with full Galois image, along with a single cubic polynomial with the same property.

In some sense $G_\infty = \mathrm{Aut}(T_\infty)$ is the expected behavior: Odoni and Juul [10, 14] show that for a generic polynomial we have $G_n = \mathrm{Aut}(T_n)$ provided that the degree of the polynomial and the characteristic of the base field are not both 2. However, it is surprisingly difficult to produce examples where this is provably the case.

There has been a recent flurry of work in this area, including [3, 11, 16], but all of these prove a slightly different version of Odoni's conjecture. Specifically, none of them provide a monic polynomial $f(x) \in \mathbb{Z}[x]$ where $G_\infty = \mathrm{Aut}(T_\infty)$. Odoni's conjecture as stated in Conjecture 1 above is still open for every composite $d \geq 4$, and we have only a single example from Looper [13] in degree 3.

We develop tools that can be used to prove polynomials do (or do not) have full Galois image. We apply these tools to the specific case $d = 4$ to see that the current techniques used in the literature are not able to prove Odoni's conjecture as stated above.

1.0.1 Outline

In Section 2.1, we construct tools that work in any degree to show full Galois image. In Section 2.2, we look at particular Kummer-2 extensions generated by discriminants and provide some conditions on the critical orbits that will force these extensions to be as large as possible. In Section 3.1, we use Newton polygons to create a tool to show quartic polynomials have full Galois image. Though we were not able to use this tool to create an example of a quartic with full image, in Section 3.2, we demonstrate that the techniques used here — which are similar to those used by Looper and other researchers — will not allow us to provide a monic quartic polynomial with integer coefficients and full arboreal Galois image. New ideas will be needed to generate these examples. In Chapter 4, we provide some conditions that force the arboreal representation to have infinite index in $\mathrm{Aut}(T_\infty)$.

CHAPTER 2
ARBOREAL SEEDLINGS

Let K be a number field and let $f(x) \in K[x]$ be a polynomial of degree $d \geq 2$. We fix the following notation to be used throughout the chapter.

- Let $\beta_1, \ldots, \beta_{d^{n-1}}$ be the roots of $f^{n-1}(x)$.
- Define M_i to be the splitting field of $f(x) - \beta_i \in \mathbb{Q}(\beta_i)$.
- Put $\delta_i = \triangle(f(x) - \beta_i)$.
- Set $L_{n-1} = K_{n-1}\left(\sqrt{\delta_1}, \ldots, \sqrt{\delta_{d^{n-1}}}\right)$, a Kummer-2 extension of K_{n-1}. We say that L_{n-1}/K_{n-1} is maximal if $\mathrm{Gal}(L_{n-1}/K_{n-1}) \cong S_2^{d^{n-1}}$.
- Define $\hat{M}_i$ to be the compositum of the fields $M_j K_{n-1}$ for $j \neq i$, i.e.,

$$\hat{M}_i = \bigvee_{j \neq i} M_j K_{n-1}.$$

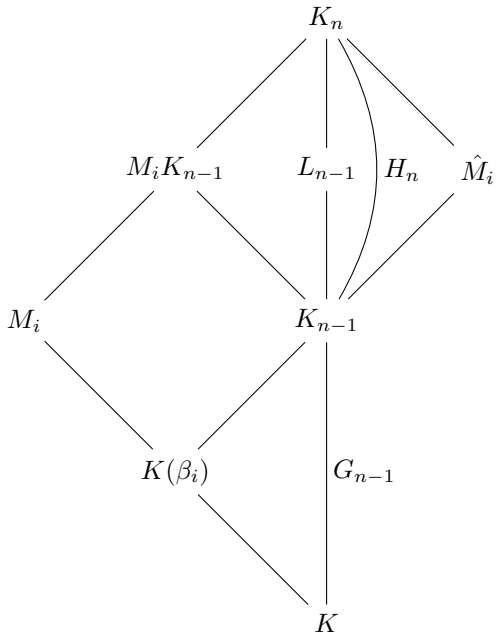

Figure 2.1: Fields between K and K_n.

2.1 Galois Toolbox

The following is inspired by [8, Section 2.2]. To show $G_\infty = \mathrm{Aut}(T_\infty)$ we will show that each of the intermediate extensions K_n/K_{n-1} is as large as possible.

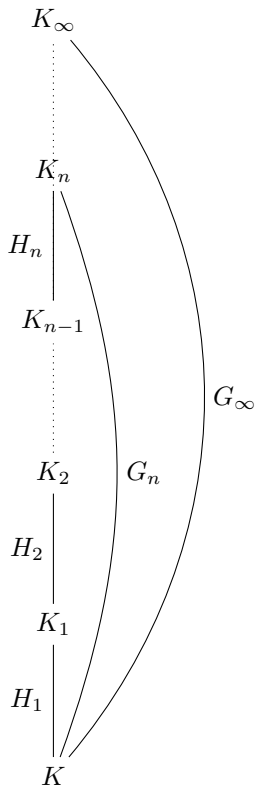

Figure 2.2: Tower of fields.

Define $H_n = \mathrm{Gal}(K_n/K_{n-1})$. Consider the restriction mapping $\mathrm{Aut}(T_n) \to \mathrm{Aut}(T_{n-1})$. We have

$$H_n \subseteq \ker(\mathrm{Aut}(T_n) \to \mathrm{Aut}(T_{n-1})) \cong (S_d)^{d^{n-1}}.$$

We say that H_n is maximal if $H_n = \ker(\mathrm{Aut}(T_n) \to \mathrm{Aut}(T_{n-1}))$. The group $G_n = \mathrm{Aut}(T_n)$ if and only if $H_1, H_2, \ldots, H_n$ are maximal. To show that $G_\infty = \mathrm{Aut}(T_\infty)$, it will suffice to show that H_n is maximal for every n.

Let T_n denote the regular d-ary rooted tree with n levels. We introduce a way to think of T_n which is inspired by [2]. The automorphism group $\mathrm{Aut}(T_n)$ of the regular rooted tree is isomorphic to the n-fold iterated wreath product $[S_d]^n$. The tree T_n can be thought of as T_{n-1} with d^{n-1} copies of

T_1 attached along the leaves of T_{n-1}. For elements $x_1, x_2, \ldots, x_{d^{n-1}} \in \mathrm{Aut}(T_1)$ and $y \in \mathrm{Aut}(T_{n-1})$, the element

$$((x_1, x_2, \ldots, x_{d^{n-1}}), y) \in \mathrm{Aut}(T_1) \wr \mathrm{Aut}(T_{n-1}) \cong \mathrm{Aut}(T_n)$$

acts on T_n by first acting on the d^{n-1} copes of T_1 by $x_1, x_2, \ldots, x_{d^{n-1}}$ respectively, and then permuting these T_1's by y.

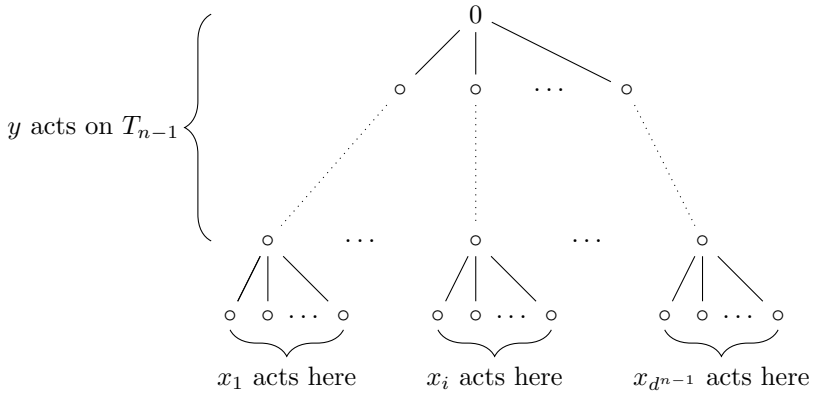

Figure 2.3: The element $((x_1, x_2, \ldots, x_{d^{n-1}}), y)$ acting on T_n.

When $\sigma \in H_n$ we have $y = \mathrm{id}$. In this case, we will simply write $\sigma = (x_1, \ldots, x_{d^{n-1}})$.

The following lemma allows us to use an element of H_n with a particular cycle type to build many other elements of H_n with the same cycle type.

Lemma 2.1.1 (Cycle Type Lemma)**.** *Let $f^{n-1}(x)$ be irreducible over K. Fix $1 \leq i, j \leq d^{n-1}$. Suppose there is a $\sigma \in H_n$ where σ is of the form*

$$\sigma = (x_1, \ldots, \mathbf{x}_i, \ldots, x_{d^{n-1}}) \in H_n \tag{2.1}$$

where $x_k \in S_d$, then there is a $\sigma_j \in H_n$ where σ_j is of the form

$$\sigma_j = (y_1, \ldots, \mathbf{y}_j, \ldots, y_{d^{n-1}}) \in H_n, \tag{2.2}$$

where there is a permutation $\rho \in S_{d^{n-1}}$ such that for each k, $y_{\rho(k)} \in S_d$ has the same cycle type as x_k, and such that $\rho(i) = j$.

Proof. Let $\alpha_{m1}, \alpha_{m2}, \ldots, \alpha_{md}$ be the roots of $f(x) - \beta_m$. Since $f^{n-1}(x)$ is irreducible, there is a

$\tau' \in G_{n-1}$ such that $\tau'(\beta_j) = \beta_i$. Extend τ' to $\tau \in G_n$. We claim that $\tau^{-1}\sigma\tau$ has the desired properties of σ_j.

Let l be arbitrary and let m be such that $\tau(\beta_l) = \beta_m$. Let $\hat{\sigma} \in S_d$ be such that $\sigma(\alpha_{mk}) = \alpha_{m\hat{\sigma}(k)}$. Notice that $\hat{\sigma}$ has the same cycle type as x_m. Let $\hat{\tau} \in S_d$ be such that $\tau(\alpha_{lk}) = \alpha_{m\hat{\tau}(k)}$. Also, $\tau^{-1}(\alpha_{mk}) = \alpha_{l\hat{\tau}^{-1}(k)}$ since $\tau\left(\alpha_{l\hat{\tau}^{-1}(k)}\right) = \alpha_{m\hat{\tau}(\hat{\tau}^{-1}(k))} = \alpha_{mk}$. So

$$\begin{aligned}\tau^{-1}\sigma\tau(\alpha_{lk}) &= \tau^{-1}\sigma\left(\alpha_{m\hat{\tau}(k)}\right)\\ &= \tau^{-1}\left(\alpha_{m(\hat{\sigma}\hat{\tau})(k)}\right)\\ &= \alpha_{l(\hat{\tau}^{-1}\hat{\sigma}\hat{\tau})(k)}.\end{aligned}$$

Therefore $\tau^{-1}\sigma\tau \in H_n$. So y_l has the same cycle type as $\hat{\tau}^{-1}\hat{\sigma}\hat{\tau}$, which has the same cycle type has $\hat{\sigma}$, which has the same cycle type as x_m. Defining ρ so that $\tau(\beta_{\rho(k)}) = \beta_k$ completes the proof. □

To apply the Cycle Type Lemma, we need to know that $f^{n-1}(x)$ is irreducible. In the sequel, we will often need to know that in fact all iterates of $f(x)$ are irreducible. The following lemma gives us an easy way to construct polynomials whose iterates are irreducible.

Lemma 2.1.2. *If $f(x)$ is a degree $d \geq 2$ polynomial that is Eisenstein at some prime p, then $f^n(x)$ is Eisenstein at p and irreducible for all $n \geq 1$.*

Proof. Let $f(x)$ be a degree $d \geq 2$ polynomial that is Eisenstein at p and write $f(x) = a_d x^d + a_{d-1}x^{d-1} + \ldots + a_2x^2 + a_1x + a_0$. Fix a $n \geq 1$ and write

$$f^n(x) = b_{d^n}x^{d^n} + b_{d^n-1}x^{d^n-1} + \ldots + b_2x^2 + b_1x + b_0.$$

Clearly, $p \mid b_i$ for $0 \leq i \leq d^n - 1$. There is an $N \geq 1$ such that $b_{d^n} = (a_d)^N$, therefore b_{d^n} is not divisible by p since a_d is not divisible by p. The constant coefficient of $f(x)$ is a fixed point of $f(x)$ $(\text{mod } p^2)$ since

$$\begin{aligned}f(a_0) &= a_d(a_0)^d + a_{d-1}(a_0)^{d-1} + \ldots + a_2(a_0)^2 + a_1(a_0) + a_0\\ &\equiv a_0 \pmod{p^2}.\end{aligned}$$

Therefore, $p^2 \nmid b_0$ since $b_0 = f^{n+1}(0) \equiv a_0 \not\equiv 0 \pmod{p^2}$. Hence, $f^n(x)$ is Eisenstein at p. □

Lemma 2.1.3 (Section 14.4, Proposition 19 in [5]). *Suppose K/F is a Galois extension and F'/F is any extension. Then KF'/F' is a Galois extension with Galois group*

$$\mathrm{Gal}(KF'/F') \cong \mathrm{Gal}(K/K \cap F')$$

isomorphic to a subgroup of $\mathrm{Gal}(K/F)$. *See Figure* 2.4.

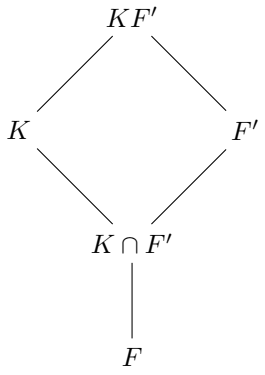

Figure 2.4: Field extensions.

Lemma 2.1.4. *Let K/F and F'/F be Galois extensions, then KF'/F' is a Galois extension and* $\mathrm{Gal}(KF'/F')$ *is a normal subgroup of* $\mathrm{Gal}(K/F)$. *See Figure* 2.5.

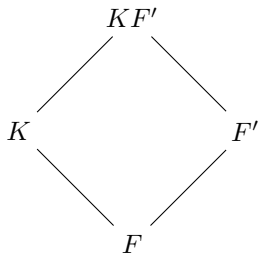

Figure 2.5: Field extensions.

Proof. By Lemma 2.1.3, KF'/F' is Galois and $\mathrm{Gal}(KF'/F') \cong \mathrm{Gal}(K/K \cap F')$. The extension $K \cap F'/F$ is Galois, therefore $\mathrm{Gal}(K/K \cap F')$ is normal in $\mathrm{Gal}(K/F)$. From the isomorphism above, we get that $\mathrm{Gal}(KF'/F')$ is normal in $\mathrm{Gal}(K/F)$. □

Recall that our overall strategy in proving $G_\infty = \mathrm{Aut}(T_\infty)$ is to show that $H_n = \mathrm{Gal}(K_n/K_{n-1})$ is maximal for every $n \geq 1$. The following lemma gives us some conditions that can be put on the

fields caught in between $K(\beta_i)$ and K_n that will force H_n to be maximal. See Figure 2.1.

Lemma 2.1.5. *Let $f(x) \in K[x]$ be a degree $d \geq 2$ polynomial and suppose $f^{n-1}(x)$ is irreducible. Suppose the following conditions are met:*

(i) There is an i where $\mathrm{Gal}(M_i/K(\beta_i)) \cong S_d$,

(ii) The extension L_{n-1}/K_{n-1} is maximal, and

(iii) The intersection $\bigcap_k \hat{M}_k \neq K_n$.

Then H_n is maximal.

Proof. If $d = 2$, then $L_{n-1} = K_n$. Therefore, condition (ii) guarantees that H_n is maximal. Assume now that $d \geq 3$. Fix an i such that $\mathrm{Gal}(M_i/K(\beta_i)) \cong S_d$. Since L_{n-1}/K_{n-1} is maximal, there is a $\sigma' \in \mathrm{Gal}(L_{n-1}/K_{n-1})$ with

$$\sigma' : \sqrt{\delta_i} \mapsto -\sqrt{\delta_i} \quad \text{and} \quad \sqrt{\delta_k} \mapsto \sqrt{\delta_k} \quad \text{for } k \neq i.$$

Lift σ' to an element $\sigma \in H_n$. The element σ is going to be of the form

$$\sigma = (\rho_1, \ldots, \rho_{i-1}, \tau_i, \rho_{i+1}, \ldots, \rho_{d^{n-1}}) \tag{2.3}$$

where $\rho_j \in A_d$ and $\tau_i \in S_d \setminus A_d$. The restriction $\sigma\big|_{M_i K_{n-1}} \in \mathrm{Gal}(M_i K_{n-1}/K_{n-1})$ is an odd permutation. By Lemma 2.1.4,

$$\mathrm{Gal}(M_i K_{n-1}/K_{n-1}) \trianglelefteq \mathrm{Gal}(M_i/K(\beta_i)) \cong S_d.$$

We have that $\mathrm{Gal}(M_i K_{n-1}/K_{n-1})$ is a normal subgroup of S_d with an odd permutation, so $\mathrm{Gal}(M_i K_{n-1}/K_{n-1}) \cong S_d$. The Cycle Type Lemma gives us that this isomorphism is true for all i.

Now set $D_i = \mathrm{Gal}(K_n/\hat{M}_i)$. Suppose that for every k we have that D_k is trivial, then $\hat{M}_k = K_n$ for all k, therefore $\bigcap \hat{M}_k = K_n$, contradicting *(iii)*. So there must be a k where D_k is nontrivial. By the Cycle Type Lemma, D_i is non-trivial for all i. By Lemma 2.1.4,

$$D_i = \mathrm{Gal}(K_n/\hat{M}_i) \trianglelefteq \mathrm{Gal}(M_i K_{n-1}/K_{n-1}) \cong S_d.$$

We will now show that $D_i \cong S_d$ by showing that D_i has an odd permutation.

For $j \neq i$, define $\hat{\rho}_j = (\mathrm{id}, \ldots, \mathrm{id}, \rho_j, \mathrm{id}, \ldots, \mathrm{id})$ where ρ_j is defined as in equation 2.3 and ρ_j occurs in the j^{th} coordinate of $\hat{\rho}_j$. Define $\hat{\sigma} = \sigma \prod_{j \neq i} {\hat{\rho}_j}^{-1}$, then

$$\hat{\sigma} = (\mathrm{id}, \ldots, \mathrm{id}, \tau_i, \mathrm{id}, \ldots, \mathrm{id}).$$

Suppose $d \geq 5$ or $d = 3$, then for each i we have that $D_i \cong A_d$ or $D_i \cong S_d$. Since $A_d \subseteq D_k$ for all k, we have that $(A_d)^{d^{n-1}} \leq H_n$ and $\hat{\rho}_j \in H_n$ for all $j \neq i$. Notice that $\hat{\sigma} \in H_n$ since $\sigma \in H_n$ and $\hat{\rho}_j \in H_n$ for all $j \neq i$. Therefore $D_i \cong S_d$ since D_i is a normal subgroup of S_d with an odd permutation.

Suppose $d = 4$, then for each i we have that $D_i \cong V_4$, or D_4, or S_4. Notice that $\rho_j^3 \in V_4$ since $\rho_j \in A_4$. Since $V_4 \subseteq D_k$ for all k, we have that $(V_4)^{d^{n-1}} \leq H_n$ and ${\hat{\rho}_j}^3 \in H_n$ for all $j \neq i$. Therefore $\hat{\sigma}^3 \in H_n$ since $\sigma \in H_n$ and ${\hat{\rho}_j}^3 \in H_n$ for all $j \neq i$. Note that τ_i^3 is an odd permutation. Therefore $D_i \cong S_4$ since D_i is a normal subgroup of S_4 with an odd permutation.

So $D_i \cong S_d$ for every d, therefore $D_k \cong S_d$ for every k by the Cycle Type Lemma. Hence, $H_n \cong (S_d)^{d^{n-1}}$ and H_n is maximal. □

The following lemma is useful for finding out when the composition of two polynomials is irreducible; it can be found in [7, Lemma 4.1].

Lemma 2.1.6 (Capelli's Lemma)**.** *Let K be a field, $f(x), g(x) \in K[x]$, and $\beta \in \overline{K}$ be a root of $g(x)$. Then $g(f(x))$ is irreducible over K if and only if both $g(x)$ is irreducible over K and $f(x) - \beta$ is irreducible over $K(\beta)$.*

Lemma 2.1.7. *Let $f(x) \in K[x]$ be a polynomial with prime degree p. Suppose for every $n \geq 1$ $f^n(x)$ is irreducible and H_n has a transposition. Then $G_\infty = \mathrm{Aut}(T_\infty)$.*

Proof. To prove the claim, we will show that $(i) - (iii)$ from Lemma 2.1.5 hold. Suppose H_n has a transposition and $f^{n-1}(x)$ is irreducible. For some i, there is a transposition in $\mathrm{Gal}(K_n/\hat{M}_i)$. Therefore $\bigcap_k \hat{M}_k \neq K_n$ and statement (iii) is true. By the Cycle Type Lemma, for every i there is an element $\sigma_i \in H_n$ of the form

$$\sigma_i = (\mathrm{id}, \ldots, \tau_i, \mathrm{id}, \ldots, \mathrm{id})$$

where τ_i is a transposition located in the i^{th} position of σ_i. Notice that

$$\sigma_i\left(\sqrt{\delta_i}\right) = -\sqrt{\delta_i} \quad \text{and} \quad \sigma_k\left(\sqrt{\delta_k}\right) = \sqrt{\delta_k} \quad \text{for } k \neq i$$

since there is an odd permutation in the i^{th} position. Define $\bar{\sigma_i} = \sigma_i\big|_{L_{n-1}} \in \mathrm{Gal}(L_{n-1}/K_{n-1})$, then the subgroup of $\mathrm{Gal}(L_{n-1}/K_{n-1})$ generated by the $\bar{\sigma_i}$ is isomorphic to $S_2^{d^{n-1}}$. Hence L_{n-1}/K_{n-1} is maximal and condition (ii) is met.

Let β_i be a root of $f^{n-1}(x)$. Since $f^n(x)$ is irreducible over $K[x]$, Capelli's Lemma gives us that $f(x) - \beta_i$ is irreducible over $K(\beta_i)$. So $\mathrm{Gal}(M_i/K(\beta_i))$ has a p-cycle and a 2-cycle, hence $\mathrm{Gal}(M_i/K(\beta_i)) \cong S_p$ and condition (i) is met. This completes the proof. □

Lemma 2.1.8. *Let $f(x)$ be a degree $d \geq 2$ polynomial and suppose $f^{n-1}(x)$ is irreducible. Suppose the following statements are true:*

(i) There is an i where $\mathrm{Gal}(M_i/K(\beta_i)) \cong S_d$.

(ii) The extension L_{n-1}/K_{n-1} is maximal.

Then for every element $x \in S_d$ there is an element in H_n of the form

$$(\rho_1, \ldots, \rho_{i-1}, x, \rho_{i+1}, \ldots, \rho_{d^{n-1}})$$

where x shows up in the i^{th} coordinate and $\rho_k \in A_d$.

Proof. Since (i) and (ii) are true, the argument at the beginning of the proof of Lemma 2.1.5 shows $\mathrm{Gal}(M_iK_{n-1}/K_{n-1}) \cong S_d$ for all i.

Since L_{n-1}/K_{n-1} is maximal, let $\sigma' \in \mathrm{Gal}(L_{n-1}/K_{n-1})$ with

$$\sigma' : \sqrt{\delta_i} \mapsto -\sqrt{\delta_i} \quad \text{and} \quad \sqrt{\delta_k} \mapsto \sqrt{\delta_k} \quad \text{for } k \neq i.$$

Lift σ' to an element $\sigma \in \mathrm{Gal}(K_n/K_{n-1}) = H_n$. The element σ is going to be of the form

$$\sigma = (\rho_1, \ldots, \rho_{i-1}, \tau_i, \rho_{i+1}, \ldots, \rho_{d^{n-1}})$$

where $\tau_i \in S_d \setminus A_d$ and $\rho_j \in A_d$. Consider the map $\pi_j : H_n \to S_d$ which takes an element $(y_1, \ldots, y_{j-1}, x_j, y_{j+1}, \ldots, y_{d^{n-1}}) \in H_n$ and maps it to x_j. Given a subset $H \subseteq H_n$, we define

$H^{(j)} = \pi_j(A)$. When S is a subgroup of G, $\langle S \rangle$ will denote the subgroup of G generated by S. Notice that $\langle H^{(i)} \rangle = \langle H \rangle^{(i)}$. Define

$$E_\sigma = \left\{ \psi^{-1}\sigma\psi : \psi \in H_n \text{ an extension of } \psi' \in \mathrm{Gal}(M_i K_{n-1}/K_{n-1}) \right\} \subseteq H_n.$$

To prove the claim, it will suffice to show $\langle E_\sigma \rangle^{(i)} \cong S_d$ and $\langle E_\sigma \rangle^{(j)} \subseteq A_d$ for every $j \neq i$.

If $j \neq i$, then $E_\sigma^{(j)}$ will consist of conjugates of ρ_j. So $\langle E_\sigma \rangle^{(j)} \subseteq A_d$ since $E_\sigma^{(j)} \subseteq A_d$. Since $\mathrm{Gal}(M_i K_{n-1}/K_{n-1}) \cong S_d$, we get that $E_\sigma^{(i)}$ contains the entire conjugacy class of the odd permutation τ_i, therefore $\langle E_\sigma \rangle^{(i)} = \langle E_\sigma^{(i)} \rangle \cong S_d$. □

Definition 2.1.9. *Let G be a group. The exponent of G, denoted $\exp(G)$, is defined to be*

$$\min\{n : g^n = e \ \forall g \in G\}.$$

Lemma 2.1.10. *Let d be of the form 2^n or $2^n + 1$, then*

$$2^{n-1} \Big|\Big| \exp(A_d).$$

Proof. Let d be of the form 2^n or $2^n + 1$. Let $\sigma \in S_d$ be a $(2, 2^{n-1})$-cycle, then $\sigma \in A_d$. Since the order of σ is 2^{n-1}, we have that $2^{n-1} \mid \exp(A_d)$. If $2^n \mid \exp(A_d)$, then that means A_d has an element of order 2^n. This can only happen of this element is a 2^n-cycle, which is an odd permutation, a contradiction. So $2^{n-1} \Big|\Big| \exp(A_d)$. □

Now we state and prove a lemma that gives us a way to remove condition (iii) of Lemma 2.1.5 if we restrict our attention to polynomials of particular degrees.

Lemma 2.1.11. *Let $f(x) \in K[x]$ be a degree $d \geq 2$ polynomial where d is of the form 2^k or $2^k + 1$ and $f^{n-1}(x)$ is irreducible. Suppose the following conditions hold:*

(i) There is an i where $\mathrm{Gal}(M_i/K(\beta_i)) \cong S_d$.

(ii) The extension L_{n-1}/K_{n-1} is maximal.

Then H_n is maximal.

Proof. From Lemma 2.1.8, there is an element $\sigma \in H_n$ which is of the form

$$\sigma = (\tau, \rho_2, \ldots, \rho_{d^{n-1}})$$

where τ is a 2^n-cycle and each $\rho_i \in A_d$. Since $2^{n-1} \big| \big| \exp(A_d)$, we have

$$\sigma^{\exp(A_d)} = (\tau^{\exp(A_d)}, \mathrm{id}, \ldots, \mathrm{id}) \in H_n.$$

Since $\tau^{\exp(A_d)}$ is $(2, 2, \ldots, 2)$-cycle, we have $\mathrm{Gal}(K_n/\hat{M}_1)$ is nontrivial, whence $\hat{M}_1 \neq K_n$. Therefore, the third condition of Lemma 2.1.5 holds, completing the proof. □

2.2 Maximal Kummer-2 Extensions and Discriminants

In this section, we explore some techniques of showing that the Kummer-2 extension L_{n-1}/K_{n-1} is maximal. We continue with all of the notation from the previous section. We use the following additional notation:

- Let $\gamma_1, \ldots, \gamma_{d-1}$ be the critical points of f.
- Let α be the leading coefficient of f.
- Let $p(y) = \triangle_x(f(x) - y)$.

From [1, Proposition 3.2], we get

$$p(y) = (-1)^{(d-1)(d-2)/2} d^d \alpha^{d-1} \prod_{i=1}^{d-1} (y - f(\gamma_i)) \in K[y]. \tag{2.4}$$

Lemma 2.2.1. *Let $f(x) \in K[x]$ be a degree $d \geq 2$ polynomial. If $G_{n-1} = \mathrm{Aut}(T_{n-1})$, then*

(i) If L_{n-1}/K_{n-1} is maximal, then $\prod_{i=1}^{d^{n-1}} \delta_i \notin K_{n-1}^{*2}$. The converse holds when d is even.

(ii) $\prod_{i=1}^{d^{n-1}} \delta_i \in K_n^{*2}$.

Proof. Recall that $\beta_1, \ldots, \beta_{d^{n-1}}$ are the roots of $f^{n-1}(x)$ and $\delta_i = \triangle(f(x) - \beta_i)$. Since $f^{n-1}(x)$ is irreducible, G_{n-1} acts transitively on the β_i.

Since $\delta_i = p(\beta_i)$ and $p(y) \in K[y]$, G_{n-1} acts transitively on the δ_i. Recall also that the field L_{n-1} is a 2-Kummer extension of K_{n-1}.

Using Kummer theory, $[L_{n-1} : K_{n-1}]$ is the order of the group D generated by the classes of δ_i in K_{n-1}^*/K_{n-1}^{*2}, where K_{n-1}^{*2} denotes the non-zero squares in K_{n-1}. We have

$$\#D = \frac{2^{d^{n-1}}}{\#V}, \text{ where } V = \left\{ (e_1, \ldots, e_{d^{n-1}}) \in \mathbb{F}_2^{d^{n-1}} : \prod_{j=1}^{d^{n-1}} \delta_j^{e_j} \in K_{n-1}^{*2} \right\}.$$

Thus V is an $\mathbb{F}_2$ vector space, and V is trivial if and only if $[L_{n-1} : K_{n-1}] = 2^{d^{n-1}}$, that is, if and only if L_{n-1}/K_{n-1} is maximal.

The transitive action of G_{n-1} on the β_i gives a transitive action on the δ_i. The action of G_{n-1} on the δ_i gives an action of G_{n-1} on V as linear transformations, making V an $\mathbb{F}_2[G_{n-1}]$ module.

By the transitivity of the action of G_{n-1} on the δ_i, the submodule $V^{G_{n-1}}$ of G_{n-1} invariant elements is not trivial if and only if $V^{G_{n-1}} = \{(0, \ldots, 0), (1, \ldots, 1)\}$. We have the following implications:

$$V^{G_{n-1}} = \{(0, \ldots, 0), (1, \ldots, 1)\} \iff (1, \ldots, 1) \in V \iff \prod_{i=1}^{d^{n-1}} \delta_i \in K_{n-1}^{*2}.$$

Suppose L_{n-1}/K_{n-1} is not maximal and d is even. Then $V \neq \{(0, 0, \ldots, 0)\}$. Since d is even, you can use any non-zero element of V to construct $(1, \ldots, 1)$, therefore $(1, \ldots, 1) \in V$. Consider the following argument of this sub-claim:

When $n = 2$, then $G_1 = \mathrm{Aut}(T_1) = S_d$. Let $v = (e_1, e_2, \ldots, e_d) \in V$ be non-zero. If $v = (1, \ldots, 1)$, then we are done. Say $v \neq (1, \ldots, 1)$. Then there is an $1 \leq i, j \leq d$ such that $e_i = 0$ and $e_j = 1$. Since $G_1 = S_d$, we have a transposition $\tau = (i, j) \in G_1$. Then $v + \tau \cdot v = (0, \ldots, 1, \ldots, 1, \ldots, 0) \in V$, where there are exactly two 1's, and they are in the i^{th} and j^{th} position.

Again, since $G_1 = S_d$, we may take $\sigma = (1, i)(2, j)$, and we have that the vector $\sigma \cdot (v + \tau \cdot v) \in V$ as well. This is the vector $w = (1, 1, 0, \ldots, 0)$, where there are exactly two 1's, and they are in the 1^{st} and 2^{nd} position. Now for each odd k, $3 \leq k < d$, define $\sigma_k \in S_d$ to be $(1, k)(2, k + 1)$. Then $\sigma_k \cdot w = (0, \ldots, 1, 1, \ldots, 0) \in V$, where the only two 1's are in the k^{th} and $(k+1)^{\text{th}}$ positions. Finally, we add: $w + \sigma_3 \cdot w + \ldots + \sigma_{d-1} \cdot w = (1, 1, \ldots, 1) \in V$.

Suppose the sub-claim is true for some $n \geq 2$, we will show it is true for $n + 1$.

Given a general $(\epsilon_1, \ldots, \epsilon_{d^n}) \in V$, imagine attaching from left to right the ϵ_i to the leaves of T_n.

For the level nodes directly above the ϵ_i, label the nodes from left to right with $\kappa_1, \ldots, \kappa_{d^{n-1}}$. See Figure 2.2.

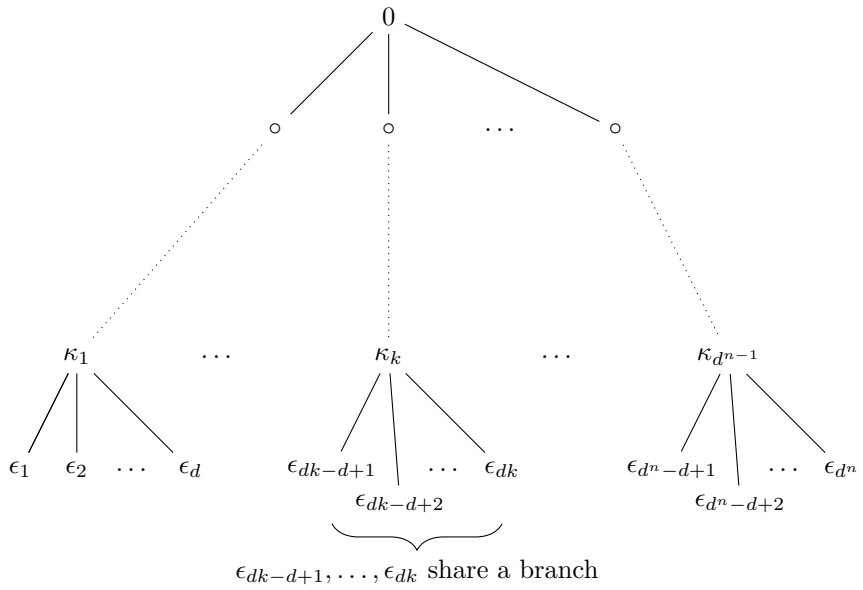

Figure 2.6: The ϵ_i and κ_j placed on T_n.

We will say that ϵ_i and ϵ_j share a branch if there is a k with $1 \leq k \leq d^{n-1}$ such that $dk-d+1 \leq i, j \leq dk$. Taking a look at Figure 2.2, for ϵ_i and ϵ_j to share it branch, this simply means there is a κ_k that is directly above them that they share. Given a κ_k, we will refer to the ϵ_i's that lie directly below κ_k, that is the ϵ_i such that $dk - d + 1 \leq i \leq dk$, as the values of κ_k. When the values of κ_k are all the same, that is when $\epsilon_i = \hat{\epsilon}$ for $dk - d + 1 \leq i \leq dk$ for some $\hat{\epsilon} \in \mathbb{F}_2$, we will associate κ_k to the value $\hat{\epsilon}$.

Suppose you apply σ to T_n for some $\sigma \in \mathrm{Aut}(T_n)$. This will result in permuting the ϵ_i's and κ_j's. Label the leaves of the permuted tree from left to right with $\epsilon'_1, \ldots, \epsilon'_{d^n}$. Since $G_n = \mathrm{Aut}(T_n)$, we have $(\epsilon'_1, \ldots, \epsilon'_{d^n}) \in V$.

Suppose $v = (e_1, \ldots, e_{d^n}) \in V$ is non-zero. If $(e_1, \ldots, e_{d^n}) = (1, \ldots, 1)$, then we are done, so suppose this is not the case. We want to show that $(1, \ldots, 1) \in V$. We will consider two cases when we set $(\epsilon_1, \ldots, \epsilon_{d^n}) = (e_1, \ldots, e_{d^n})$: (1) There is a k where the values of κ_k are not all the same, and (2) For every k, the values of κ_k are all the same.

(Case 1) Suppose there is a k where the values of κ_k are not all the same. Then there is an i and j with $dk - d + 1 \leq i, j \leq dk$ such that $e_i = 1$ and $e_j = 0$. Since ϵ_i and ϵ_j share a branch and

$G_n = \mathrm{Aut}(T_n)$, we have $\tau = (i, j) \in G_n$. Then $v + \tau \cdot v = (0, \ldots, 1, \ldots, 1, \ldots, 0) \in V$ has exactly two 1's in the i^{th} and j^{th} place. Since $G_n = \mathrm{Aut}(T_n)$, there is a map $\sigma \in G_n$ such that $\sigma(i) = 1$ and $\sigma(j) = 2$. Then $\sigma \cdot (v + \tau \cdot v) \in V$. This is the vector $w = (1, 1, 0, \ldots, 0)$ where there are exactly two 1's in the 1^{st} and 2^{nd} position. For every odd k, there is a map $\sigma_k \in G_n$ such that $\sigma_k(1) = k$ and $\sigma_k(2) = k + 1$. Then $\sigma_k \cdot w = (0, \ldots, 1, 1, \ldots, 0)$ where there are exactly two 1's in the k^{th} and $(k+1)^{\text{th}}$ position. Finally, we add: $w + \sigma_3 \cdot w + \ldots + \sigma_{d^n-1} \cdot w = (1, 1, \ldots, 1) \in V$.

(Case 2) Suppose for every k, the values of κ_k are all the same. For $1 \leq k \leq d^{n-1}$, let $\hat{\epsilon}_k$ be such that the values of κ_k are $\hat{\epsilon}_k$. See Figure 2.2.

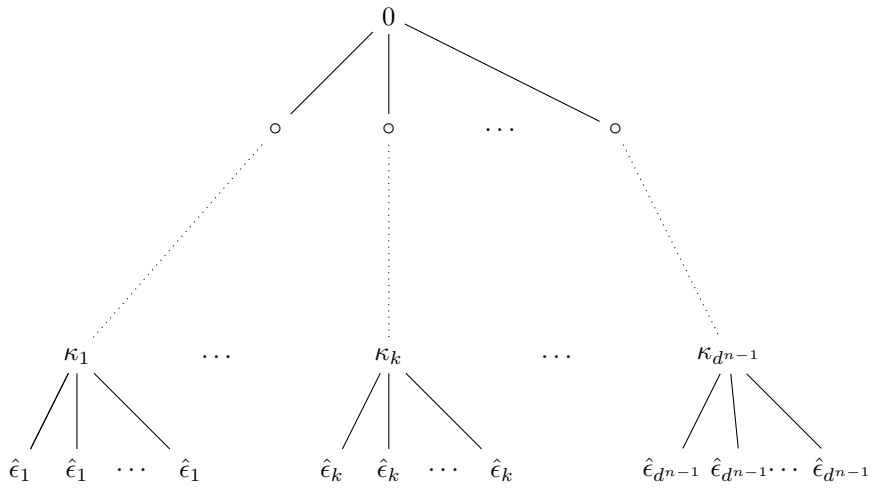

Figure 2.7: For each k, the values of κ_k are the same.

Notice that v is invariant under the action of any element of the kernel of the restriction mapping $\mathrm{Aut}(T_n) \to \mathrm{Aut}(T_{n-1})$. So given a $\sigma = ((x_1, \ldots, x_{d^{n-1}}), \tau) \in \mathrm{Aut}(T_n)$ for $x_i \in \mathrm{Aut}(T_1)$ and $\tau \in \mathrm{Aut}(T_{n-1})$, the action of σ on v is determined by τ.

Let $V' = \{(f_1, \ldots, f_{d^{n-1}}) \in \mathbb{F}_2^{d^{n-1}}\}$ where V' is an $\mathbb{F}_2[G_{n-1}]$ module. Set $v' = (\hat{\epsilon}_1, \ldots, \hat{\epsilon}_{d^{n-1}}) \in V'$. By the inductive hypothesis, we can use v' to build $(1, \ldots, 1) \in V'$. Therefore, we can use v to build $(1, \ldots, 1) \in V$.

So $(1, \ldots, 1) \in V$, so from the chain earlier, we have $\prod \delta_i \in K_{n-1}^{*2}$.

Suppose $\prod \delta_i \in K_{n-1}^{*2}$. Then $(1, \ldots, 1) \in V$, so $V \neq \{(0, 0, \ldots, 0)\}$. Therefore, L_{n-1}/K_{n-1} is maximal. This proves the first claim. The fact that $\prod \delta_i \in K_n^{*2}$ follows from $\sqrt{\delta_i} \in L_{n-1} \leq K_n$ for every i. $\square$

Now that we've established that $\prod \delta_i$ is an important quantity, let's get a better understanding

of it.

Definition 2.2.2. *Let $g \in K[x]$ be a polynomial. We define the quantity $\ell(g) \in K$ to be the leading coefficient of g.*

Lemma 2.2.3. *Let $f(x) \in K[x]$. If $\alpha = \ell(f)$, then $\ell(f^n) = \alpha^{\frac{d^n-1}{d-1}}$.*

Proof. We will proceed with induction on n. The case for $n = 1$ quickly follows since $\ell(f) = \alpha = \alpha^{\frac{d-1}{d-1}}$. Now suppose $\ell(f^n) = \alpha^{(d^n-1)/(d-1)}$ some $n \geq 1$, then

$$\begin{aligned}
\ell(f^{n+1}(x)) &= \ell(f^n \circ f) \\
&= \ell\left(\alpha^{\frac{d^n-1}{d-1}}(f(x))^{d^n}\right) && \text{since } \ell(f^n) = \alpha^{(d^n-1)/(d-1)} \\
&= \alpha^{\frac{d^n-1}{d-1}}\alpha^{d^n} \\
&= \alpha^{\frac{d^{n+1}-1}{d-1}}. && \square
\end{aligned}$$

Definition 2.2.4. *Let $x, y \in K^*$. If there is a $z \in K^*$ such that $x = z^2 y$, then we will write $x \sim y$.*

Definition 2.2.5. *Let $a, b \in \mathbb{Z}$ and let $m \geq 2$. Define*

$$[a \equiv_m b] = \begin{cases} 1 & a \equiv b \pmod{m} \\ 0 & a \not\equiv b \pmod{m}. \end{cases}$$

We prove some basic properties about Definition 2.2.4 and 2.2.5.

Lemma 2.2.6. *Let K be a field and let $\sim$ be the relation on K defined by Definition* 2.2.4. *Then*

(i) The relation $\sim$ is an equivalence relation,

(ii) $x^n \sim x^{(n \mod 2)}$,

(iii) If $x \sim y$, then $x \in K_n^{*2}$ if and only if $y \in K_n^{*2}$.

Proof. (i) Let $a \in K$ and set $z = 1$. Then $a = z^2 a$, therefore $a \sim a$. So $\sim$ is reflexive. Suppose $a \sim b$, then there is a non-zero $z \in K$ such that $a = z^2 b$. By inverting z, we get that $b \sim a$. Therefore $\sim$ is symmetric. Suppose $a \sim b$ and $b \sim c$, then there is a $z_1, z_2 \in K$ such that $a = z_1^2 b$ and $b = z_2^2 c$. Setting $z = z_1 z_2$ gives us that $a \sim c$. Therefore $\sim$ is transitive and is an equivalence relation.

(ii) Let $k = n \pmod 2$ and write $n = 2m + k$ for some $m \in \mathbb{Z}$. Define $z = x^m$, then

$$x^n = x^{2m+k} = (x^m)^2 x^k = z^2 x^{(n \mod 2)}.$$

(iii) Let $x \sim y$ and let $z \in K$ be the non-zero element such that $x = z^2 y$. If $y \in K_n^{*2}$, then $x \in K_n^{*2}$ since $z^2 \in K_n^{*2}$. □

Let $\gamma_0, \ldots, \gamma_{d-1}$ be the critical points of $f(x)$. Define

$$\Gamma_n = \prod_{i=1}^{d-1} f^n(\gamma_i). \tag{2.5}$$

Lemma 2.2.7. *Let $f(x) \in K[x]$ be a degree $d \geq 2$ polynomial. Let $\alpha = \ell(f)$, put*

$$B_n = \begin{cases} (-1)^{[d \equiv_4 3]} d^{[d \equiv_2 1]} \alpha^{[d \equiv_2 0]} & n \geq 2 \\ (-1)^{[d \equiv_4 2,3]} d^{[d \equiv_2 1]} \alpha^{[d \equiv_2 0]} & n = 1, \end{cases}$$

and set $D_n = B_n \Gamma_n$. If $G_{n-1} = \mathrm{Aut}(T_{n-1})$, then

(i) If L_{n-1}/K_{n-1} is maximal, then $D_n \notin K_{n-1}^{*2}$. The converse holds when d is even.

(ii) $D_n \in K_n^{*2}$.

Proof. Let $\beta_1, \ldots, \beta_{d^{n-1}}$ be the roots of $f^{n-1}(x)$. Notice that

$$f^{n-1}(x) = \ell(f^{n-1}) \prod_{i=1}^{d^{n-1}} (x - \beta_i). \tag{2.6}$$

Recall $\delta_i = \triangle(f(x) - \beta_i)$. To prove the claim, by Lemma 2.2.1, it will suffice to show $D_n \sim \prod_{i=1}^{d^{n-1}} \delta_i$.

Fix $n \geq 2$, then

$$\begin{aligned}
\prod_{i=1}^{d^{n-1}} \delta_i &= \prod_{i=1}^{d^{n-1}} p(\beta_i) && \text{equation (2.4)} \\
&= \prod_{i=1}^{d^{n-1}} (-1)^{(d-1)(d-2)/2} d^d \alpha^{d-1} \prod_{j=1}^{d-1} (\beta_i - f(\gamma_j)) \\
&= ((-1)^{(d-1)(d-2)/2} d^d \alpha^{d-1})^{d^{n-1}} \prod_{i=1}^{d^{n-1}} \prod_{j=1}^{d-1} (\beta_i - f(\gamma_j)) \\
&\sim ((-1)^{(d-1)(d-2)/2} d^d \alpha^{d-1})^{d} (-1)^{d^{n-1}(d-1)} \prod_{j=1}^{d-1} \prod_{i=1}^{d^{n-1}} (f(\gamma_j) - \beta_i) \\
&\sim ((-1)^{(d-1)(d-2)/2} d^d \alpha^{d-1})^{d} \prod_{j=1}^{d-1} \frac{f^{n-1}(f(\gamma_j))}{\ell(f^{n-1})} && \text{equation (2.6)} \\
&= (-1)^{d(d-1)(d-2)/2} d^{d^2} \alpha^{d^2-d} \prod_{j=1}^{d-1} \frac{f^n(\gamma_j)}{\alpha^{\frac{d^{n-1}-1}{d-1}}} && \text{Lemma 2.2.3} \\
&\sim \frac{(-1)^{d^2(d-1)/2} d^d}{\alpha^{d^{n-1}-1}} \Gamma_n \\
&\sim \frac{(-1)^{d^2(d-1)/2} d^d}{\alpha^{d-1}} \Gamma_n.
\end{aligned}$$

Since $[d^2(d-1)/2 \equiv_2 1] = 1$ if and only if $d \equiv 3 \pmod 4$, we get

$$\prod_{i=1}^{d^{n-1}} \delta_i \sim (-1)^{[d \equiv_4 3]} d^{[d \equiv_3 1]} \alpha^{[d \equiv_2 0]} \Gamma_n = B_n \Gamma_n.$$

Now let $n = 1$. The quantity $\prod \delta_i$ is the discriminant of $f(x)$, so

$$\begin{aligned}
\triangle(f(x)) &= p(0) \\
&= (-1)^{(d-1)(d-2)/2} d^d \alpha^{d-1} \prod_{i=1}^{d-1} (-f(\gamma_i)) \\
&= (-1)^{(d-1)(d-2)/2} d^d \alpha^{d-1} (-1)^{d-1} \Gamma_n \\
&= (-1)^{d(d-1)/2} d^d \alpha^{d-1} \Gamma_n.
\end{aligned}$$

Since $[d(d-1)/2 \equiv_2 1] = 1$ if and only if $d \equiv 2, 3 \pmod 4$, we get

$$\triangle(f(x)) \sim (-1)^{[d \equiv_4 2,3]} d^{[d \equiv_2 1]} \alpha^{[d \equiv_2 0]} \Gamma_n = B_1 \Gamma_n. \quad \square$$

The following gives us a way to compute the discriminant of the iterates of $f(x)$.

Lemma 2.2.8 (Lemma 2.6 from [7]). *Let $f, g \in K[x]$ where f and g have respectively degrees d_f, d_g and let $\gamma_1, \gamma_2, \ldots, \gamma_{d-1}$ be the critical points of f. Put $\triangle_n = \mathrm{Disc}(g \circ f^n)$. Then for all $n \geq 1$ we have*

$$\triangle_n = \pm \triangle_{n-1}^{d_f} d_f^{k_1} \ell(f)^{k_2} \ell(g)^{k_3} \prod_{i=1}^{d-1} g(f^n(\gamma_i)),$$

where $k_1 = d_g d_f^n$, $k_2 = d_g^2 d_f^{2n-1}$, and $k_3 = d_f - 1$.

We specialize Lemma 2.2.8 to get a formula specific to the discriminant of the iterates of monic polynomials.

Lemma 2.2.9. *Let $f(x) \in K[x]$ be a degree $d \geq 2$ monic polynomial, then for every $n \geq 1$ we have*

$$\triangle(f^n(x)) = \pm d^{d^n} \triangle(f^{n-1}(x))^d \prod_{i=1}^{d-1} f^n(\gamma_i)$$

where $\gamma_1, \ldots, \gamma_{d-1}$ are the critical points of $f(x)$.

Proof. Define $g(x) = x$, then $d_g = 1$. Also $d_f = d$, $\ell(f) = 1$, and $\ell(g) = 1$, therefore $k_1 = d_g d_f^n = d^n$ and

$$\begin{aligned}
\triangle(f^n(x)) &= \triangle_n \\
&= \pm \triangle_{n-1}^{d_f} d_f^{k_1} \ell(f)^{k_2} \ell(g)^{k_3} \prod_{i=1}^{d-1} g(f^n(\gamma_i)) \\
&= \pm \triangle_{n-1}^{d} d^{d^n} \prod_{i=1}^{d-1} f^n(\gamma_i) \\
&= \pm d^{d^n} \triangle \left(f^{n-1}(x)\right)^d \prod_{i=1}^{d-1} f^n(\gamma_i).
\end{aligned}$$

□

The next lemma relates the following quantities: $\triangle_n$, D_n and Γ_n. We use $\mathbb{Z}_{(p)}$ to denote the integers localized at (p).

Lemma 2.2.10 (Discriminant Lemma). *Let $f(x) \in \mathbb{Z}_{(p)}[x]$ be a monic polynomial of degree $d \geq 2$ with $p \nmid d$. Then $v_p(\Gamma_n) = v_p(D_n)$ and*

$$v_p(\triangle_n) = \sum_{k=1}^{n} d^{n-k} v_p(\Gamma_k) = \sum_{k=1}^{n} d^{n-k} v_p(D_k).$$

Proof. Since $D_n = \pm d^{[d \equiv_2 1]}\Gamma_n$ we get $v_p(D_n) = v_p(\Gamma_n)$. To finish the proof, it will suffice to show that $v_p(\triangle_n) = \sum_{k=1}^{n} d^{n-k} v_p(\Gamma_k)$. We will proceed with induction on n.

If $n = 1$, then we want to show that $v_p(\triangle_1) = v_p(\Gamma_1)$. This follows from the fact that $\triangle(f(x)) = \pm d^d a_1$. Now suppose that the statement is true for some $n \geq 1$, then

$$\begin{aligned}
v_p(\triangle_{n+1}) &= v_p\left(\pm d^{d^{n+1}} \triangle(f^n(x))^d \prod_{i=1}^{d-1} f^{n+1}(\gamma_i)\right) \\
&= v_p\left(\pm d^{d^{n+1}} \triangle(f^n(x))^d \Gamma_{n+1}\right) \\
&= d v_p(\triangle_n) + v_p(\Gamma_{n+1}) \\
&= d \sum_{k=1}^{n} d^{n-k} v_p(\Gamma_k) + v_p(\Gamma_{n+1}) && \text{inductive hypothesis} \\
&= \sum_{k=1}^{n} d^{n+1-k} v_p(\Gamma_k) + v_p(\Gamma_{n+1}) \\
&= \sum_{k=1}^{n+1} d^{n+1-k} v_p(\Gamma_k). && \square
\end{aligned}$$

Lemma 2.2.11. *Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial with even degree $d \geq 2$. Fix an $n \geq 1$. Suppose $G_{n-1} = \mathrm{Aut}(T_{n-1})$. If there is a $p \nmid d$ such that $v_p(\Gamma_n)$ is odd and $v_p(\Gamma_k) = 0$ for every k with $1 \leq k < n$, then L_{n-1}/K_{n-1} is maximal.*

Proof. Let $p \nmid d$. To prove the claim, we will apply Lemma 2.2.7 by showing $D_n \notin K_{n-1}^{*2}$ for every $n \geq 1$.

Let $n = 1$ and suppose $v_p(\Gamma_1)$ is odd. By the Discriminant Lemma we have $v_p(D_1) = v_p(\Gamma_1)$ which is odd, so D_1 is not a square in $K_0 = \mathbb{Q}$.

Now suppose $n \geq 2$ and suppose $v_p(\Gamma_n)$ is odd and $v_p(\Gamma_k) = 0$ for every k with $1 \leq k < n$. By the Discriminant Lemma $v_p(\triangle_{n-1}) = \sum_{k=1}^{n-1} d^{n-1-k} v_p(\Gamma_k) = 0$, so p does not ramify in K_{n-1}.

Let $\mathfrak{P}$ be a prime lying above p in K_{n-1}. Since p does not ramify in K_{n-1}, $v_{\mathfrak{P}}(x) = v_p(x)$ for every $x \in \mathbb{Q}$. So $v_{\mathfrak{P}}(D_n)$ is odd since $v_{\mathfrak{P}}(D_n) = v_p(D_n) = v_p(\Gamma_n)$ and $v_p(\Gamma_n)$ is odd. So $D_n \notin K_{n-1}^{*2}$ and hence L_{n-1}/K_{n-1} is maximal. $\square$

2.3 Newton Polygons

As we have seen, a common way to construct irreducible polynomials is by constructing polynomials that are Eisenstein at a prime. In this section, we introduce a tool to construct irreducible

polynomials which extends the idea of being Eisenstein at a prime. To do this, we use Newton polygons.

Definition 2.3.1. *Let K be a number field and $\mathfrak{P}$ a prime in K. Consider the points*

$$A = \{(i, v_{\mathfrak{P}}(a_i)) : 0 \leq i \leq d\} \cup \{(0, \infty), (d, \infty)\}.$$

Let $C(A)$ denote the convex hull of A. We call $C(A)$ the Newton polygon of $f(z)$. The set $C(A)$ is bounded below by ℓ line segments $L_1, L_2, \ldots, L_\ell$ which we call the line segments of the Newton Polygon of $f(z)$.

Example 2.3.1. *Let $f(x) = x^5 + 3x^2 - 27x + 27$. The set A and the line segments of the Newton polygon at $p = 3$ are pictured in Figure* 2.8.

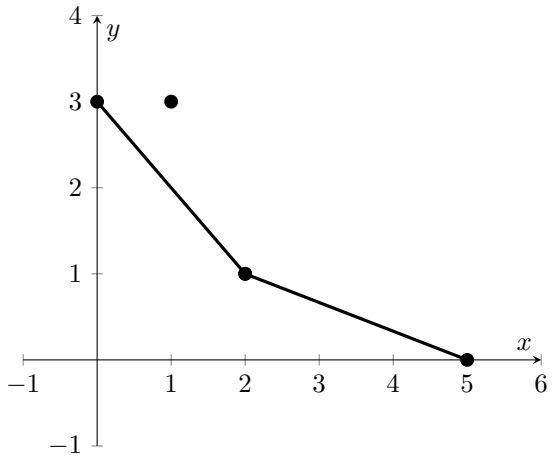

Figure 2.8: Newton polygon of $f(x) = x^5 + 3x^2 - 27x + 27$ at $p = 3$.

Example 2.3.2. *Let $f(x) = x^3 + 4x^2 + 16x + 16$. The set A and the line segments of the Newton polygon at $p = 2$ are pictured in Figure* 2.9.

We define $\mathbb{C}_p$ to be the completion of the algebraic closure of the p-adic field $\mathbb{Q}_p$. Koblitz describes how we can relate the slope and the horizontal length of the line segments of Newton polygons to the p-adic valuation of a polynomial's roots.

Proposition 2.3.2 (Section 3, Lemma 4 from [12])**.** *If $f \in \mathbb{C}_p[z]$ is a polynomial, and the Newton polygon of f includes a line segment of slope m whose horizontal length is N, then $f(z)$ has exactly N roots α (counted with multiplicity), satisfying $v_p(\alpha) = -m$.*

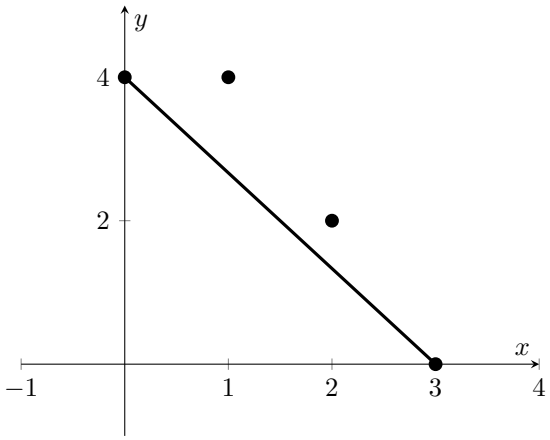

Figure 2.9: Newton polygon of $f(x) = x^3 + 4x^2 + 16x + 16$ at $p = 2$.

Let's revisit Example 2.3.1. The line segments L_1 and L_2 have slopes -1 and $\frac{-1}{3}$ respectively. By Theorem 2.3.2, since the horizontal length of L_1 is 2, there are two roots α of $f(x)$ satisfying $v_3(\alpha) = 1$. Similarly, since the horizontal length of L_2 is 3, there are three roots β of $f(x)$ satisfying $v_3(\beta) = \frac{1}{3}$.

Now, let's revisit Example 2.3.1. The Newton polygon of $f(x)$ has only one line segment with slope $\frac{-4}{3}$ with width 3, so all 3 roots of $f(x)$ satisfy $v_2(\alpha) = \frac{4}{3}$ by Theorem 2.3.2. Let $\alpha_1, \alpha_2, \alpha_3$ be the roots of $f(x)$. If $f(x)$ is reducible over $\mathbb{Q}[x]$, then $\alpha_i\alpha_j \in \mathbb{Q}$ for some $i \neq j$. Since $v_2(x) \in \mathbb{Z}$ for all $x \in \mathbb{Q}$ and $v_2(\alpha_i\alpha_j) = \frac{8}{3} \notin \mathbb{Z}$, $f(x)$ is irreducible over $\mathbb{Q}[x]$.

Let K be a number field. Since there is an embedding $K \hookrightarrow \mathbb{C}_p$, a similar statement to the previous theorem holds when we replace $\mathbb{C}_p$ with a number field K and p with a prime $\mathfrak{P}$ in K.

Lemma 2.3.3. *Let K be a number field and $\mathfrak{P}$ a prime in K. If $f \in K[x]$ is a polynomial, and the Newton polygon of f with respect to $\mathfrak{P}$ includes a line segment of slope m whose horizontal length is N, then $f(z)$ has exactly N roots $\alpha \in \bar{K}$ (counted with multiplicity), satisfying $v_{\mathfrak{P}}(\alpha) = -m$.*

Proof. Let $L_{1,\mathfrak{P}}, \ldots, L_{\ell,\mathfrak{P}}$ be the line segments of the Newton polygon of f with respect to $\mathfrak{P}$. For each i, let $m_{i,\mathfrak{P}}$ and $N_{i,\mathfrak{P}}$ be the slope and horizontal length of $L_{i,\mathfrak{P}}$ respectively.

Let p be a prime in $\mathbb{Q}$ such that $\mathfrak{P} \mid p$. Let $e = e(\mathfrak{P}/p)$ be the ramification index of $\mathfrak{P}$. Since $v_{\mathfrak{P}}(x) = ev_p(x)$, the Newton polygon of f with respect to $\mathfrak{P}$ can be constructed by taking the Newton polygon of f with respect to p and scaling it vertically by a factor of e.

Let $L_{1,p}, \ldots, L_{\ell,p}$ be the line segments of the Newton polygon of f with respect to p. Let $m_{i,p}$ and $N_{i,p}$ be the slope and horizontal length of $L_{i,p}$ respectively. From our comments above, we have

$m_{i,\mathfrak{P}} = em_{i,p}$ and $N_{i,\mathfrak{P}} = N_{i,p}$.

Fix an i. From Theorem 2.3.2, $f(z)$ has $N_{i,p}$ roots α satisfying $v_p(\alpha) = -m_{i,p}$. For such a root α,

$$v_{\mathfrak{P}}(\alpha) = ev_p(\alpha) = -em_{i,p} = -m_{i,\mathfrak{P}}.$$

Therefore, $f(z)$ has $N_{i,\mathfrak{P}} = N_{i,p}$ roots α satisfying $v_p(\alpha) = -m_{i,\mathfrak{P}}$. □

Using ideas from Example 2.3.2, we state and prove an irreducibility criterion for Newton polygons.

Lemma 2.3.4. *Let K be a number field, $\mathfrak{P}$ a prime in K, and $f(x) \in K[x]$ a degree $d \geq 1$ polynomial. If the Newton Polygon of f at $\mathfrak{P}$ has only one line segment with slope $\frac{-a}{d}$ and $(a, d) = 1$, then f is irreducible over $K[x]$.*

Proof. Let $\alpha_1, \ldots, \alpha_d$ be the roots of $f(x)$. For every i, $v_{\mathfrak{P}}(\alpha_i) = \frac{a}{d}$ and $(a, d) = 1$. For each proper subset $I \subseteq \{i : 1 \leq i \leq d\}$, define $A_I = \prod_{i\in I}^{k} \alpha_i$ and $f_I(x) = \prod_{i\in I}(x - \alpha_i)$. Notice that $f(x)$ is reducible over $K[x]$ if and only if there is a proper subset $I \subsetneq \{i : 1 \leq i \leq d\}$ such that $f_I \in K[x]$, implying that $A_I \in K$. Let I be such that $f_I \in K[x]$. We have $v_{\mathfrak{P}}(A_I) = \dfrac{\#(I) \cdot a}{d}$.

Recall $v_{\mathfrak{P}}(x) \in \mathbb{Z}$ for every $x \in K$. So $\#(I) = d$ since $A_I \in K$, $\frac{\#(I)\cdot a}{d} \in \mathbb{Z}$, and $(a, d) = 1$. Hence, $f_I = cf$ for some $c \in K$, and $f(x)$ is irreducible over $K[x]$. □

The following corollary shows that the Eisenstein test for irreducibility is a special case of this Newton polygon irreducibility.

Corollary 2.3.5. *Let K be a number field, $\mathfrak{P}$ a prime in K, and $f(x) \in K[x]$ a degree $d \geq 2$ polynomial. If $f(x)$ is Eisenstein at $\mathfrak{P}$, then $f(x)$ is irreducible over $K[x]$.*

Proof. Write

$$f(x) = a_d x^d + a_{d-1}x^{d-1} + \ldots + a_1 x + a_0.$$

Since $f(x)$ is Eisenstein at $\mathfrak{P}$, we get $v_{\mathfrak{P}}(a_0) = 1$, $v_{\mathfrak{P}}(a_d) = 0$, and $v_{\mathfrak{P}}(a_i) \geq 1$ for $1 \leq i < d$. See Figure 2.10.

The Newton polygon of $f(x)$ consists of a single line segment with slope $\frac{-1}{d}$. Since $(1, d) = 1$, $f(x)$ is irreducible over $K[x]$ by Lemma 2.3.4. □

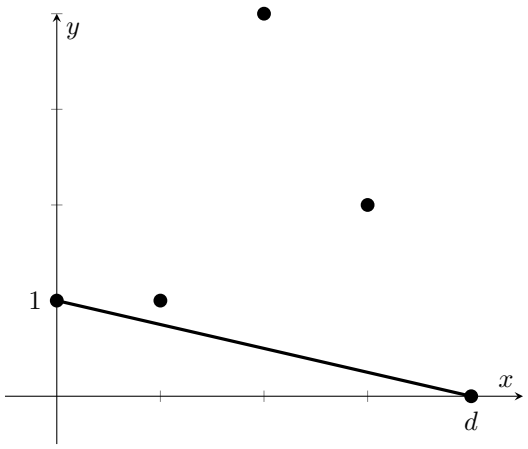

Figure 2.10: Newton Polygon when Eisenstein at $\mathfrak{P}$.

CHAPTER 3
DEGREE 4

Proofs of Odoni's Conjecture [3, 11, 16] provide examples in each degree of polynomials in $\mathbb{Q}[x]$ (or $K[x]$ for number field K) such that $G_\infty = \mathrm{Aut}(T_\infty)$. None of these examples, however, are monic polynomials in $\mathbb{Z}[x]$. In this chapter, we show that it is in fact impossible to find a monic quartic polynomial in $\mathbb{Z}[x]$ for which the techniques used in these papers can be used to show $G_\infty = \mathrm{Aut}(T_\infty)$. We begin by developing general tools for quartic polynomials.

3.1 Newton Polygons and Irreducibility of Cubic Resolvents

Let $f(x) \in \mathbb{Q}[x]$ be a monic degree 4 polynomial. From Lemma 2.1.5 we saw that if we want to show $G_\infty = \mathrm{Aut}(T_\infty)$, it is necessary that for every n there is a root β_i of $f^{n-1}(x)$ such that

$$\mathrm{Gal}(M_i/\mathbb{Q}(\beta_i)) \cong S_4.$$

Recall M_i is the splitting field of $f(x) - \beta_i$ over $\mathbb{Q}(\beta_i)$. From [5, Page 615], it suffices to show

(i) $f(x) - \beta_i$ is irreducible over $\mathbb{Q}(\beta_i)$

(ii) $\delta_i = \triangle(f(x) - \beta_i)$ is not a square in $\mathbb{Q}(\beta_i)$

(iii) the cubic resolvent of $f(x) - \beta_i$ is irreducible over $\mathbb{Q}(\beta_i)$.

We have seen that condition (i) is satisfied provided that $f(x)$ is Eisenstein at some prime. Condition (ii) will follow when L_{n-1}/K_{n-1} is maximal. In this section, our focus will be to discover some simple conditions on the coefficients of $f(x)$ that will imply that the cubic resolvent of $f(x)-\beta_i$ is irreducible over $\mathbb{Q}(\beta_i)$. The main tool we use is Lemma 2.3.4.

Lemma 3.1.1. *Let K be a number field, $g(x) \in K[x]$ a monic cubic polynomial, and $\mathfrak{P}$ a prime K. Write $g(x) = x^3 + a_2x^2 + a_1x + a_0$. Suppose the following conditions hold:*

$$\frac{2}{3}v_{\mathfrak{P}}(a_0) \leq v_{\mathfrak{P}}(a_1) \tag{3.1}$$

$$\frac{1}{3}v_{\mathfrak{P}}(a_0) \leq v_{\mathfrak{P}}(a_2) \tag{3.2}$$

$$v_{\mathfrak{P}}(a_0) \not\equiv 0 \pmod 3. \tag{3.3}$$

Then $g(x)$ is irreducible over $K[x]$.

Proof. To show that $g(x)$ is irreducible over $K[x]$, we will take a look at the shape of the Newton polygon of $g(x)$ at $\mathfrak{P}$.

Consider the points $A = \{(i, v_{\mathfrak{P}}(a_i)) : i = 0, 1, 2, 3\}$ where $a_3 = 1$. Let L be the line connecting $(0, v_{\mathfrak{P}}(a_0))$ and $(3, 0)$. The equation of line L is

$$y = \frac{-v_{\mathfrak{P}}(a_0)}{3}x + v_{\mathfrak{P}}(a_0) = \left(1 - \frac{x}{3}\right) v_{\mathfrak{P}}(a_0).$$

If all the points of A are not below the line L and $v_{\mathfrak{P}}(a_0)$ is relatively prime to 3, then the shape of the Newton polygon of $g(x)$ at the prime $\mathfrak{P}$ will confirm that $g(x)$ is irreducible over $K[x]$. By assumption (3.3), $v_{\mathfrak{P}}(a_0)$ is relatively prime to 3. All the points of A are not below the line L provided that we show $\left(1 - \frac{i}{3}\right) v_{\mathfrak{P}}(a_0) \leq v_{\mathfrak{P}}(a_i)$ for $0 \leq i \leq 3$. Notice that this inequality is true for $i = 0$ and $i = 3$. Assumptions (3.1) and (3.2) take care of the cases $i = 1$ and $i = 2$. □

Definition 3.1.2. *Let K be a number field, $g(x) \in K[x]$ a cubic polynomial, and p a prime in $\mathbb{Q}$. Write $g(x) = x^3 + a_2x^2 + a_1x + a_0$. We say that $g(x)$ is Newton irreducible at p over K if there is a prime $\mathfrak{P}$ in K lying over p such that conditions* (3.1)*,* (3.2)*, and* (3.3) *are satisfied from Lemma* 3.1.1.

It follows directly from Lemma 3.1.1 that if $g(x)$ is Newton irreducible at p over K, then $g(x)$ is irreducible over $K[x]$.

Let $f(x) = x^4 + ax^3 + bx^2 + cx + d \in \mathbb{Q}[x]$ be Eisenstein at p. Whenever we mention the cubic resolvent of $f(x)$, we will be referring to one of the following cubic polynomials:

$$R_1(f(x)) = x^3 - bx^2 + (ac - 4d)x - (a^2d + c^2 - 4bd) \tag{3.4}$$

$$R_2(f(x)) = x^3 - 2bx^2 + (b^2 + ac - 4d)x + (a^2d + c^2 - abc). \tag{3.5}$$

Definition 3.1.3. *Let $f(x) \in \mathbb{Q}[x]$ be a monic quartic polynomial that is Eisenstein at p. We say that $f(x)$ is Newton irreducible at p if there is a $j \in \{1, 2\}$ where for every $n \geq 2$ and every root β of $f^{n-1}(x)$, the cubic resolvent $R_j(f(x) - \beta)$ is Newton irreducible at p over $\mathbb{Q}(\beta)$.*

Now that we have laid out the definitions of Newton irreducibility, we state and prove a lemma to convince the reader that Newton irreducibly is a worthwhile idea to study when you are trying to show that $G_\infty = \mathrm{Aut}(T_\infty)$ for quartic polynomials.

Proposition 3.1.4. *Let $f(x) \in \mathbb{Q}[x]$ be a monic quartic polynomial that is Eisenstein at p and suppose the cubic resolvent of $f(x)$ is irreducible over $\mathbb{Q}[x]$. If $f(x)$ is Newton irreducible at p and L_{n-1}/K_{n-1} is maximal for every $n \geq 1$, then $G_\infty = \mathrm{Aut}(T_\infty)$.*

Proof. Let $f(x)$ be Eisenstein at p and suppose the cubic resolvent of $f(x)$ is irreducible over $\mathbb{Q}[x]$. Suppose $f(x)$ is Newton irreducible at p and L_{n-1}/K_{n-1} is maximal for every $n \geq 1$.

Let $n = 1$. Since L_0/K_0 is maximal, we get that $\triangle(f(x))$ is not a square in $\mathbb{Q}$. Since $f(x)$ is Eisenstein at p, we get that $f(x)$ is irreducible over $\mathbb{Q}[x]$. Since the cubic resolvent of $f(x)$ is irreducible over $\mathbb{Q}[x]$, we have that $\mathrm{Gal}(K_1/\mathbb{Q}) \cong S_4$ and H_1 is maximal.

Since $f(x)$ is Newton irreducible, there is a $1 \leq j \leq 2$ where for every $n \geq 2$ and every root β of $f^{n-1}(x)$, the cubic resolvent $R_j(f(x) - \beta)$ is Newton irreducible at p over $\mathbb{Q}(\beta)$. Fix a $n \geq 2$ and a root β_i of $f^{n-1}(x)$. By Lemma 3.1.1, $R_j(f(x) - \beta_i)$ is irreducible over $\mathbb{Q}(\beta_i)$. Since $f(x)$ is Eisenstein at p, $f^n(x)$ is Eisenstein at p and irreducible, therefore $f(x) - \beta_i$ is irreducible over $\mathbb{Q}(\beta_i)$ by Capelli's Lemma. Since L_{n-1}/K_{n-1} is maximal, we get that $\delta_i = \triangle(f(x) - \beta_i)$ is not a square in K_{n-1}, therefore δ_i is not a square in $\mathbb{Q}(\beta_i)$. Therefore $\mathrm{Gal}(M_i/\mathbb{Q}(\beta_i)) \cong S_4$. By Lemma 2.1.11 we get that H_n is maximal for every $n \geq 1$. Hence $G_\infty = \mathrm{Aut}(T_\infty)$. □

When showing a cubic polynomial is Newton irreducible, it is required that you have some information on the p-adic valuation of the coefficients.

Lemma 3.1.5. *Let $f(x) \in \mathbb{Q}[x]$ be quartic polynomial that is Eisenstein at p and let β be a root of $f^{n-1}(x)$ where $n \geq 2$. Let $\mathfrak{P}$ be a prime lying above p in $\mathbb{Q}(\beta)$. Then $v_{\mathfrak{P}}(\beta) = 1$ and $v_{\mathfrak{P}}(x) = 4^{n-1}v_p(x)$ for every $x \in \mathbb{Q}$.*

Proof. The polynomial $f^{n-1}(x)$ is Eisenstein at p since $f(x)$ is Eisenstein at p. Therefore, by [4, Theorem 3.1 and Corollary 3.5], p totally ramifies in $\mathbb{Q}(\beta)$, $v_{\mathfrak{P}}(\beta) = 1$, and $e(\mathfrak{P}/p) = \deg(f^{n-1}(x)) = 4^{n-1}$. If $x \in \mathbb{Q}$, then $v_{\mathfrak{P}}(x) = e(\mathfrak{P}/p)v_p(x) = 4^{n-1}v_p(x)$. □

Lemma 3.1.6. *Let $f(x) = x^4 + ax^3 + bx^2 + cx + d \in \mathbb{Q}[x]$ be Eisenstein at p. If $f(x)$ is Newton irreducible at p, then $p = 2$.*

Proof. Let $f(x)$ be Eisenstein at p and Newton irreducible at p. Let $n \geq 2$ and let β be a root of $f^{n-1}(x)$. Let $\mathfrak{P}$ be a prime lying above p in $\mathbb{Q}(\beta)$. By Lemma 3.1.5, $v_{\mathfrak{P}}(\beta) = 1$ and $v_{\mathfrak{P}}(x) = 4^{n-1}v_p(x)$ for every $x \in \mathbb{Q}$.

Suppose for a contradiction that $p \neq 2$. Let $g(x)$ be a cubic resolvent of $f(x) - \beta$ and write $g(x) = x^3 + a_2x^2 + a_1x + a_0$. From equation (3.4) and equation (3.5), $g(x)$ will be one of the following cubic polynomials:

$$R_1(f(x) - \beta) = x^3 - bx^2 + (ac - 4(d - \beta))x - (c^2 + (a^2 - 4b)(d - \beta))$$
$$R_2(f(x) - \beta) = x^3 - 2bx^2 + (b^2 + ac - 4(d - \beta))x + (a^2(d - \beta) + c^2 - abc).$$

Notice a_1 is one of the following values:

$$a_1 = ac - 4(d - \beta) \tag{3.6}$$
$$a_1 = b^2 + ac - 4(d - \beta). \tag{3.7}$$

Since f is Eisenstein at p, $v_p(a), v_p(b), v_p(c) \geq 1$ and $v_p(d) = 1$. By Lemma 3.1.5, we have $v_{\mathfrak{P}}(a), v_{\mathfrak{P}}(b), v_{\mathfrak{P}}(c) \geq 4^{n-1}$ and $v_{\mathfrak{P}}(d) = 4^{n-1}$. Assume a_1 satisfies equation (3.6), then $v_{\mathfrak{P}}(a_1) \geq \min\{v_{\mathfrak{P}}(ac), v_{\mathfrak{P}}(4(d - \beta)\}$ with equality when they are not equal. But $v_{\mathfrak{P}}(ac) = v_{\mathfrak{P}}(a) + v_{\mathfrak{P}}(c) \geq 2 \cdot 4^{n-1}$. Since $p \neq 2, v_{\mathfrak{P}}(4) = 0$, so $v_{\mathfrak{P}}(4(d - \beta)) = 0 + \min\{v_{\mathfrak{P}}(d), v_{\mathfrak{P}}(\beta)\} = 1$. We conclude $v_{\mathfrak{P}}(a_1) = 1$. A similar calculation gives the same conclusion when a_1 satisfies equation (3.7). Furthermore, a_0 is one of the following values:

$$a_0 = -(c^2 + (a^2 - 4b)(d - \beta))$$
$$a_0 = a^2(d - \beta) + c^2 - abc.$$

Similar calculations to the ones above give $v_{\mathfrak{P}}(a_0) \geq 4^{n-1}$. By equation (3.1) in Lemma 3.1.1 we have

$$\frac{2}{3}4^{n-1} \leq \frac{2}{3}v_{\mathfrak{P}}(a_0) \leq v_{\mathfrak{P}}(a_1) = 1.$$

This inequality is false for all $n \geq 2$, therefore $f(x)$ is not Newton irreducible at $p \neq 2$. Hence $p = 2$. □

For the rest of this section, we will frequently use the following equivalences: Let $0 < \epsilon < 1$ and $x, y \in \mathbb{Z}$. Then

(i) $x \leq y + \epsilon \iff x < y + \epsilon \iff x \leq y$

(ii) $x + \epsilon \leq y \iff x + \epsilon < y \iff x + 1 \leq y$.

The next four lemmas develop a simple condition for the resolvent cubic of $f(x) - \beta_i$ to be Newton irreducible at 2 over $\mathbb{Q}(\beta_i)$ based just on the coefficients of f. Lemmas 3.1.7 and 3.1.8 deal with when we take the resolvent cubic to be R_1, and Lemmas 3.1.7 and 3.1.8 deal with R_2. The conclusion in both cases is the same: The cubic resolvent of $f(x) - \beta_i$ is Newton irreducible at 2 over $\mathbb{Q}(\beta_i)$ if and only if $v_2(c) = 1$.

Lemma 3.1.7. *Let $f(x) = x^4 + ax^3 + bx^2 + cx + d$ be Eisenstein at 2 and let β be a root of $f^{n-1}(x)$ where $n \geq 2$. Let $g(x) = R_1(f(x) - \beta)$ and write $g(x) = x^3 + a_2x^2 + a_1x + a_0$. Let $\mathfrak{P}$ be a prime lying above 2 in $\mathbb{Q}(\beta)$. Then*

$$v_{\mathfrak{P}}(a_2) = 4^{n-1}v_2(b) \tag{3.8}$$

$$v_{\mathfrak{P}}(a_1) = \begin{cases} 2 \cdot 4^{n-1} + 1 & \text{if } 3 \leq v_2(a) + v_2(c) \\ 2 \cdot 4^{n-1} & \text{if } v_2(a) = v_2(c) = 1 \end{cases} \tag{3.9}$$

$$v_{\mathfrak{P}}(a_0) = \begin{cases} 2 \cdot 4^{n-1}v_2(c) & \text{if } 2v_2(c) \leq v_2(a^2 - 4b) \\ 4^{n-1}v_2(a^2 - 4b) + 1 & \text{if } 2v_2(c) \geq v_2(a^2 - 4b) + 1. \end{cases} \tag{3.10}$$

Note: Since the polynomial is Eisenstein at 2, if $v_2(a) + v_2(c) < 3$, then necessarily $v_2(a) = v_2(b) = 1$.

Proof. By Lemma 3.1.5, $v_{\mathfrak{P}}(\beta) = 1$ and $v_{\mathfrak{P}}(x) = 4^{n-1}v_p(x)$ for every $x \in \mathbb{Q}$. Equation (3.4) gives

$$g(x) = R_1(f(x) - \beta) = x^3 - bx^2 + (ac - 4(d - \beta))x - (c^2 + (a^2 - 4b)(d - \beta)).$$

Therefore

$$\begin{aligned} a_2 &= -b \\ a_1 &= ac - 4(d - \beta) \\ a_0 &= -(c^2 + (a^2 - 4b)(d - \beta)). \end{aligned}$$

Equation (3.8) directly follows.

We now turn to equation (3.9). Since $v_{\mathfrak{P}}(ac) = 4^{n-1}(v_2(a)+v_2(c))$ and $v_{\mathfrak{P}}(4(d-\beta)) = 2\cdot 4^{n-1}+1$, we have $v_{\mathfrak{P}}(a_1) = v_{\mathfrak{P}}(ac-4(d-\beta)) \geq \min\{4^{n-1}(v_2(a)+v_2(c)), 2\cdot 4^{n-1}+1\}$ with equality when they are not equal. These values are not equal since they are not equal modulo 2, hence

$$v_{\mathfrak{P}}(a_1) = \min\{4^{n-1}(v_2(a)+v_2(c)), 2\cdot 4^{n-1}+1\}. \tag{3.11}$$

We see that $v_{\mathfrak{P}}(a_1) = 2\cdot 4^{n-1}+1$ if and only if $2\cdot 4^{n-1}+1 < 4^{n-1}(v_2(a)+v_2(c))$. A straightforward calculation shows this is equivalent to $3 \leq v_2(a)+v_2(c)$, confirming equation (3.9).

Now we turn to equation (3.10). Notice that $v_{\mathfrak{P}}(c^2) = 2\cdot 4^{n-1}v_2(c)$ and $v_{\mathfrak{P}}((a^2-4b)(d-\beta)) = 4^{n-1}v_2(a^2-4b)+1$. Therefore $v_{\mathfrak{P}}(a_0) = v_{\mathfrak{P}}(c^2+(a^2-4b)(d-\beta)) \geq \min\{2\cdot 4^{n-1}v_2(c), 4^{n-1}v_2(a^2-4b)+1\}$ with equality when they are not equal. These values are not equal since they are not equal modulo 2, provided $a_0 \neq 0$. In this case

$$v_{\mathfrak{P}}(a_0) = \min\{2\cdot 4^{n-1}v_2(c), 4^{n-1}v_2(a^2-4b)+1\}. \tag{3.12}$$

We see that $v_{\mathfrak{P}}(a_0) = 2\cdot 4^{n-1}v_2(c)$ if and only if $2\cdot 4^{n-1}v_2(c) < 4^{n-1}v_2(a^2-4b)+1$. A straightforward calculation shows this is equivalent to $2v_2(c) \leq v_2(a^2-4b)$, confirming equation (3.10). If $a_0 = 0$, necessarily $c = a^2-4b = 0$, and equation (3.10) holds in this case as well. □

Lemma 3.1.8. *Let $f(x) = x^4+ax^3+bx^2+cx+d$ be Eisenstein at 2. Then $R_1(f(x)-\beta)$ is Newton irreducible at 2 over $\mathbb{Q}(\beta)$ for every root β of $f^{n-1}(x)$ for every $n \geq 2$ if and only if $v_2(c) = 1$.*

Proof. Let $n \geq 2$. Let β be a root of $f^{n-1}(x)$ and let $g(x) = R_1(f(x)-\beta)$. Write $g(x) = x^3+a_2x^2+a_1x+a_0$. For the rest of the proof, when we say that $g(x)$ is Newton irreducible we mean that $g(x)$ is Newton irreducible at 2 over $\mathbb{Q}(\beta)$. For simplicity, we will define the following cases:

Case A: $3 \leq v_2(a)+v_2(c)$	Case C: $2v_2(c) \leq v_2(a^2-4b)$
Case B: $v_2(a) = v_2(c) = 1$	Case D: $2v_2(c) \geq v_2(a^2-4b)+1$.

By Lemma 3.1.7 $v_{\mathfrak{P}}(a_2) = 4^{n-1}v_2(b)$ and

$$v_{\mathfrak{P}}(a_1) = \begin{cases} 2\cdot 4^{n-1}+1 & \text{Case A} \\ 2\cdot 4^{n-1} & \text{Case B,} \end{cases} \qquad v_{\mathfrak{P}}(a_0) = \begin{cases} 2\cdot 4^{n-1}v_2(c) & \text{Case C} \\ 4^{n-1}v_2(a^2-4b)+1 & \text{Case D.} \end{cases}$$

Since $f(x)$ is Eisenstein at 2, we have the following fact that we will use throughout:

$$v_2(a^2 - 4b) \geq 2. \tag{3.13}$$

($\Longleftarrow$) Suppose $v_2(c) = 1$. We want to show that $R_1(f(x) - \beta)$ is Newton irreducible at 2 over $\mathbb{Q}(\beta)$. Since $v_2(c) = 1$, case C holds by (3.13). First, we will show that $g(x)$ is Newton irreducible when $v_2(a) = 1$. Then we show that $g(x)$ is Newton irreducible when $v_2(a) \geq 2$.

Suppose $v_2(a) = 1$, so case B holds.

- Combining case B and C with condition (3.1), we have $\frac{2}{3} \cdot 2 \cdot 4^{n-1} v_2(c) \leq 2 \cdot 4^{n-1}$. This statement holds since $v_2(c) = 1$.
- Combining case C with condition (3.2), we have $\frac{1}{3} \cdot 2 \cdot 4^{n-1} v_2(c) \leq 4^{n-1} v_2(b)$. This statement holds since $v_2(c) = 1$ and $v_2(b) \geq 1$.
- Combining case C with condition (3.3), we have $2 \cdot 4^{n-1} v_2(c) \not\equiv 0 \pmod 3$. Once again, this statement holds since $v_2(c) = 1$.

Now suppose $v_2(a) \geq 2$, so case A holds.

- Combining case A and C with condition (3.1), we have $\frac{2}{3} \cdot 2 \cdot 4^{n-1} v_2(c) \leq 2 \cdot 4^{n-1} + 1$. A straightforward calculation shows that this inequality is equivalent to $v_2(c) = 1$.
- Combining case C with condition (3.2), we have $\frac{1}{3} \cdot 2 \cdot 4^{n-1} v_2(c) \leq 4^{n-1} v_2(b)$. This statement holds since $v_2(c) = 1$.
- Combining case C with condition (3.3), we have $2 \cdot 4^{n-1} v_2(c) \not\equiv 0 \pmod 3$. Once again, this statement holds since $v_2(c) = 1$.

Hence, when $v_2(c) = 1$, we get that $R_1(f(x) - \beta)$ is Newton irreducible.

($\Longrightarrow$) Now, suppose $v_2(c) \geq 2$, so case A holds. We want to show $R_1(f(x) - \beta)$ is not Newton irreducible. Suppose for a contradiction that $R_1(f(x) - \beta)$ is Newton irreducible. We showed above that when you combine case A and C with condition (3.1), you get statement which is equivalent to $v_2(c) = 1$, a contradiction. It remains only to consider the combination of case A and case D.

- Combining condition (3.1) with case A and D, we have $\frac{2}{3}\left(4^{n-1}v_2(a^2-4b)+1\right) \leq 2\cdot 4^{n-1}+1$. A straightforward calculation shows this is equivalent to

$$v_2(a^2-4b) \leq 3. \tag{3.14}$$

- Combining condition (3.3) with case D, we have $4^{n-1}v_2(a^2-4b)+1 \not\equiv 0 \pmod 3$. A straightforward calculation shows this is equivalent to $v_2(a^2-4b) \not\equiv 2 \pmod 3$. Combining this with condition (3.13) and (3.14), we conclude that

$$v_2(a^2-4b) = 3. \tag{3.15}$$

- Combining condition (3.2) with case D, we have $\frac{1}{3}\left(4^{n-1}v_2(a^2-4b)+1\right) \leq 4^{n-1}v_2(b)$. A straightforward calculation shows this is equivalent to

$$4 \leq v_2(4b). \tag{3.16}$$

Since $v_2(a^2)$ is even and $v_2(a^2) \geq 2$, condition (3.16) implies (3.15) is false.

Hence, $R_1(f(x)-\beta)$ is Newton irreducible if and only if $v_2(c)=1$. □

Lemma 3.1.9. *Let $f(x)=x^4+ax^3+bx^2+cx+d$ be Eisenstein at 2 and let β be a root of $f^{n-1}(x)$ where $n \geq 2$. Let $g(x)=R_2(f(x)-\beta)$ and write $g(x)=x^3+a_2x^2+a_1x+a_0$. Let $\mathfrak{P}$ be a prime lying above 2 in $\mathbb{Q}(\beta)$. Then*

$$v_{\mathfrak{P}}(a_2) = 4^{n-1}(1+v_2(b)) \tag{3.17}$$

$$v_{\mathfrak{P}}(a_1) = \begin{cases} 2\cdot 4^{n-1}+1 & \text{if } v_2(b^2+ac) \geq 3 \\ 2\cdot 4^{n-1} & \text{if } v_2(b^2+ac)=2 \end{cases} \tag{3.18}$$

$$v_{\mathfrak{P}}(a_0) = \begin{cases} 2\cdot 4^{n-1}v_2(a)+1 & \text{if } v_2(c)+v_2(c-ab) \geq 2v_2(a)+1 \\ 4^{n-1}(v_2(c)+v_2(c-ab)) & \text{if } v_2(c)+v_2(c-ab) \leq 2v_2(a). \end{cases} \tag{3.19}$$

Proof. By Lemma 3.1.5, $v_{\mathfrak{P}}(\beta)=1$ and $v_{\mathfrak{P}}(x)=4^{n-1}v_2(x)$ for every $x \in \mathbb{Q}$. Equation (3.5) gives

$$g(x)=R_2(f(x)-\beta)=x^3-2bx^2+(b^2+ac-4(d-\beta))x+(a^2(d-\beta)+c^2-abc).$$

Therefore

$$a_2 = -2b$$
$$a_1 = b^2 + ac - 4(d - \beta), \text{ and}$$
$$a_0 = a^2(d - \beta) + c^2 - abc.$$

Equation (3.17) directly follows. We now turn to equation (3.18). Since $v_{\mathfrak{P}}(b^2+ac) = 4^{n-1}v_2(b^2+ac)$ and $v_{\mathfrak{P}}(4(d-\beta)) = 2 \cdot 4^{n-1} + 1$, we have $v_{\mathfrak{P}}(a_1) = v_{\mathfrak{P}}(b^2 + ac - 4(d-\beta)) \geq \min\{4^{n-1}v_2(b^2+ac), 2 \cdot 4^{n-1} + 1\}$, with equality when they are not equal. These values are not equal since they are not equal modulo 2, hence

$$v_{\mathfrak{P}}(a_1) = \min\{4^{n-1}v_2(b^2 + ac), 2 \cdot 4^{n-1} + 1\}. \tag{3.20}$$

We see that $v_{\mathfrak{P}}(a_1) = 2 \cdot 4^{n-1} + 1$ if and only if $4^{n-1}v_2(b^2 + ac) > 2 \cdot 4^{n-1} + 1$. A straightforward computation shows this is equivalent to $v_2(b^2 + ac) \geq 3$, confirming equation (3.18).

Since $v_{\mathfrak{P}}(a^2(d-\beta)) = 2 \cdot 4^{n-1}v_2(a) + 1$ and $v_{\mathfrak{P}}(c^2 - abc) = 4^{n-1}(v_2(c) + v_2(c - ab))$, we get that $v_{\mathfrak{P}}(a_0) = v_{\mathfrak{P}}(a^2(d-\beta) + c^2 - abc) \geq \min\{2 \cdot 4^{n-1}v_2(a) + 1, 4^{n-1}(v_2(c) + v_2(c-ab))\}$, with equality when they are not equal. These values are not equal since they are not equal modulo 2, provided $a_0 \neq 0$. In this case

$$v_{\mathfrak{P}}(a_0) = \min\{2 \cdot 4^{n-1}v_2(a) + 1, 4^{n-1}(v_2(c) + v_2(c - ab))\}. \tag{3.21}$$

We see that $v_{\mathfrak{P}}(a_0) = 2 \cdot 4^{n-1}v_2(a) + 1$ if and only if $4^{n-1}(v_2(c) + v_2(c-ab)) > 2 \cdot 4^{n-1}v_2(a) + 1$. A straightforward computation shows this is equivalent to $v_2(c) + v_2(c-ab) \geq 2v_2(a) + 1$, confirming equation (3.19). If $a_0 = 0$, necessarily $a = c = 0$, so equation (3.19) holds in this case as well. □

Lemma 3.1.10. *Let $f(x) = x^4 + ax^3 + bx^2 + cx + d$ be Eisenstein at 2. Then $R_2(f(x) - \beta)$ is Newton irreducible at 2 for every root β of $f^{n-1}(x)$ for every $n \geq 2$ if and only if $v_2(c) = 1$.*

Proof. Let $n \geq 2$. Let β be a root of $f^{n-1}(x)$, and let $g(x) = R_2(f(x) - \beta)$. Write $g(x) = x^3 + a_2x^2 + a_1x + a_0$. For the rest of the proof, when we say that $g(x)$ is Newton irreducible we mean

that $g(x)$ is Newton irreducible at 2 over $\mathbb{Q}(\beta)$. For simplicity, we will define the following cases:

$$\begin{aligned} &\text{Case A: } v_2(b^2+ac) \geq 3 && \text{Case C: } v_2(c)+v_2(c-ab) \geq 2v_2(a)+1 \\ &\text{Case B: } v_2(b^2+ac) = 2 && \text{Case D: } v_2(c)+v_2(c-ab) \leq 2v_2(a). \end{aligned}$$

By Lemma 3.1.9 we get $v_{\mathfrak{P}}(a_2) = 4^{n-1}(1+v_2(b))$ and

$$v_{\mathfrak{P}}(a_1) = \begin{cases} 2\cdot 4^{n-1}+1 & \text{Case A} \\ 2\cdot 4^{n-1} & \text{Case B,} \end{cases} \qquad v_{\mathfrak{P}}(a_0) = \begin{cases} 2\cdot 4^{n-1}v_2(a)+1 & \text{Case C} \\ 4^{n-1}(v_2(c)+v_2(c-ab)) & \text{Case D.} \end{cases}$$

First, we show that if $g(x)$ is Newton irreducible, then case C does not hold. Suppose, for a contradiction, $g(x)$ is Newton irreducible and case C holds. Combining case C with condition (3.3), we have $2\cdot 4^{n-1}v_2(a)+1 \not\equiv 0 \pmod 3$. A straightforward calculation shows this is equivalent to

$$v_2(a) \not\equiv 1 \pmod 3. \tag{3.22}$$

We will show that a contradiction is reached when assuming case A or B holds.

Suppose case A holds. Combining case A and C with condition (3.1), we have $\frac{2}{3}(2\cdot 4^{n-1}v_2(a)+1) \leq 2\cdot 4^{n-1}+1$. A straightforward calculation shows that this is equivalent to $v_2(a)=1$, contradicting condition (3.22).

Now, suppose case B holds. Combining case B and C with condition (3.1), we have $\frac{2}{3}(2\cdot 4^{n-1}v_2(a)+1) \leq 2\cdot 4^{n-1}$. A straightforward calculation shows that this is equivalent to $v_2(a)=1$, contradicting condition (3.22).

Hence, if $g(x)$ is Newton irreducible, then case case C does not hold. Now, we turn to proving the statement of the lemma.

($\Longrightarrow$) Suppose $v_2(c) \geq 2$. We will show $g(x)$ not Newton irreducible. Suppose for a contradiction $g(x)$ is Newton irreducible. From the discussion above, we have case C does not hold. Hence, case D holds.

Notice $v_2(c-ab) \geq \min\{v_2(c), v_2(ab)\}$. Each of those are at least 2, so $v_2(c-ab) \geq 2$ as well. Therefore

$$v_2(c)+v_2(c-ab) \geq 4. \tag{3.23}$$

We show that assuming case A or B hold leads to a contradiction.

Suppose case A holds. Combining case A and case D with condition (3.1), we have $\frac{2}{3}\cdot 4^{n-1}(v_2(c)+v_2(c-ab)) \leq 2\cdot 4^{n-1}+1$. A straightforward calculations shows this is equivalent to $v_2(c)+v_2(c-ab) \leq 3$, contradicting equation (3.23).

Now, suppose case B holds. Combining case B and D with condition (3.1), we have $\frac{2}{3}\cdot 4^{n-1}(v_2(c)+v_2(c-ab)) \leq 2\cdot 4^{n-1}$. A straightforward calculations shows this is equivalent to $v_2(c)+v_2(c-ab) \leq 3$, once again, contradicting equation (3.23).

Hence, $g(x)$ is not Newton irreducible when $v_2(c) \geq 2$.

($\Longleftarrow$) Suppose $v_2(c) = 1$. Case D holds since

$$v_2(c-ab) = 1. \tag{3.24}$$

Combining case D with condition (3.2), we have $\frac{1}{3}\cdot 4^{n-1}(v_2(c)+v_2(c-ab)) \leq 4^{n-1}(1+v_2(b))$. Combining equation (3.24) with the facts that $v_2(c) = 1$ and $v_2(b) \geq 1$, we see condition (3.2) holds.

Combining case D with condition (3.3), we have $4^{n-1}(v_2(c)+v_2(c-ab)) \not\equiv 0 \pmod 3$. This condition holds since $v_2(c) = 1$.

To finish proving the claim we will show that if case A or B hold, then $g(x)$ is Newton irreducible. In each case, we only need to check that condition (3.1) holds.

- Combining case A and D with condition (3.1), we have $\frac{2}{3}\cdot 4^{n-1}(v_2(c)+v_2(c-ab)) \leq 2\cdot 4^{n-1}+1$. This condition holds since $v_2(c) = 1$ and $v_2(c-ab) = 1$.
- Combining case B and D with condition (3.1), we have $\frac{2}{3}\cdot 4^{n-1}(v_2(c)+v_2(c-ab)) \leq 2\cdot 4^{n-1}$. This condition holds since $v_2(c) = 1$ and $v_2(c-ab) = 1$.

Hence, if $v_2(c) = 1$, then $g(x)$ is Newton irreducible. □

The following lemma follows directly from Lemma 3.1.8 and 3.1.10.

Lemma 3.1.11. *Let $f(x) = x^4+ax^3+bx^2+cx+d$ be Eisenstein at 2. Then $f(x)$ is Newton irreducible at 2 if and only if $v_2(c) = 1$.*

Proposition 3.1.12. *Let $f(x) \in \mathbb{Q}[x]$ be a monic degree 4 polynomial that is Eisenstein at 2 and suppose the cubic resolvent of $f(x)$ is irreducible over $\mathbb{Q}[x]$. Write $f(x) = x^4+ax^3+bx^2+cx+d$. If L_{n-1}/K_{n-1} is maximal for all $n \geq 1$ and $v_2(c) = 1$, then $G_\infty = \mathrm{Aut}(T_\infty)$.*

Proof. By Lemma 3.1.11, $f(x)$ is Newton irreducible at 2. Since L_{n-1}/K_{n-1} is maximal for all n and the cubic resolvent of $f(x)$ is irreducible over $\mathbb{Q}[x]$, we have that $G_\infty = \mathrm{Aut}(T_\infty)$ by Proposition 3.1.4. □

3.2 Limitations in Degree 4

In the literature on arboreal Galois representations [8, 9, 13, 17], common techniques have come up repeatedly, with modifications introduces by Looper to allow them to apply in degrees greater than 2. However, all the work on the general version of Odoni's conjecture for composite degrees has re framed the conjecture, no longer requiring monic polynomials in $\mathbb{Z}[x]$. In this section, we show that in fact the techniques used in these papers cannot provide a monic quartic polynomial over $\mathbb{Z}[x]$ that has full arboreal Galois image. We begin by briefly describing the common pieces of these proofs.

In all the cases, the proof that the iterates of f^n is irreducible follows from the polynomial itself being Eisenstein at some prime. There is no other method in the literature to show this crucial step. Even the potentially simpler problem that the iterates f^n are "eventually stable"(there is an absolute bound B such that f^n has at most B factors) seems out of reach.

For quadratic polynomials, proving that H_n is maximal at each step required finding a transposition in H_n. To show that H_n is maximal, provided that $f^{n-1}(x)$ is irreducible, it was enough to demonstrate the existence of an odd prime p such that $v_p(f^n(\gamma_0)))$ is odd and $v_p(f^j(\gamma_0))) = 0$ for all $1 \leq j < n$. The technique used in each case was the same: If 0 is strictly periodicity for f, then by reducing the values of $f^n(\gamma_0)$ modulo p, we see that (for almost all primes p) if $p \mid f^j(\gamma_0)$, then $p \nmid f^k(\gamma_0)$ for all $k < j$. This guaranteed that for almost every prime p, a prime p dividing $f^n(\gamma_0)$ has never divided any previous term of the sequence. To get the odd valuation, the authors use reduction modulo m to see that the value is never a perfect square, forcing $v_p(f^n(\gamma_0))$ to be odd for some p. The results for higher degrees use slight modifications of these techniques, and still relied on the examples having 0 as strictly preperiodic point to get a transposition in the Galois group.

For higher degrees, an additional piece is required to demonstrate that H_n is maximal: There needs to be a d-cycle in $\mathrm{Gal}(M_i/K(\beta_i))$ where β is some root of f^{n-1}. The techniques here were a bit more haphazard, and often depended on the particular form of the examples cooked up by the authors. For example, Looper uses trinomials, and Benedetto and Juul use polynomials of the form $x^d - bx^m$ with explicit conditions on d and m.

A more general attack in degree 4 would be using the cubic resolvent, as demonstrated in Section 3.1. Unfortunately, if we want to construct a monic quartic $f(x) \in \mathbb{Z}[x]$ with $G_\infty = \mathrm{Aut}(T_\infty)$, it will be impossible if we use the common assumptions listed above along with Newton irreducibility. This means that a genuinely new idea is needed to prove the version of Odoni's conjecture stated in Conjecture 1 when $d = 4$.

Proposition 3.2.1. *There are no examples of monic quartic polynomials $f(x) \in \mathbb{Z}[x]$ that are Eisenstein at 2, Newton irreducible 2, and for which $z = 0$ is preperiodic.*

To prove this, we use Rice's classification of monic integer polynomials where zero is preperiodic.

Proposition 3.2.2 (Proposition 2.1 from [15])**.** *Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial such that the orbit of 0 under f is finite. Then*

(i) $f(0) = 0$, *and* $f(x) = xP(x)$ *for some monic polynomial* $P(x)$.

(ii) $f(0) = k$ *and* $f(k) = 0$ *for some nonzero* $k \in \mathbb{Z}$, *therefore*

$f(x) = (x - k)(xP(x) - 1)$ *for some monic polynomial* $P(x)$.

(iii) $f(0) = k$ *and* $f(k) = k$ *for some nonzero* $k \in \mathbb{Z}$, *therefore*

$f(x) = (x - k)xP(x) + k$ *for some monic* $P(x)$.

(iv) $f(0) = 1$, $f(1) = k$, *and* $f(k) = 1$ *for some nonzero* $k \in \mathbb{Z}$, *therefore*

$f(x) = x(x - k)((x - 1)P(x) - 1) + 1$ *for some monic* $P(x)$.

(v) $f(0) = -1$, $f(-1) = k$, *and* $f(k) = -1$ *for some nonzero* $k \in \mathbb{Z}$, *therefore*

$f(x) = x(x - k)((x + 1)P(x) + 1) - 1$ *for some monic (or zero)* $P(x)$.

(vi) All iterates $f^n(0)$, $n \geq 1$, *are* ± 1 *or* ± 2.

Proof of Proposition 3.2.1. Let $f(x)$ be a monic integer polynomial and write $f(x) = x^4 + ax^2 + bx^2 + cx + d$. Suppose the orbit of 0 under f is finite. Then at least one of (i) – (vi) from Proposition 3.2.2 is true.

Let $f(x)$ be Eisenstein at 2 and Newton irreducible at 2, then $f(x)$ is irreducible and $f(0) \neq \pm 1$. Furthermore, $v_2(c) = 1$ by Lemma 3.1.11. Since $f(x)$ is irreducible, statements (i) and (ii) from Proposition 3.2.2 are false. Since $f(0) \neq \pm 1$, statements (iv) and (v) from Proposition 3.2.2 are false. Therefore, statement (iii) or (vi) from Proposition 3.2.2 hold.

Suppose statement (iii) from Proposition 3.2.2 is true. Then there is a nonzero $k \in \mathbb{Z}$ such that $f(0) = k$ and $f(k) = k$. From a straightforward computation, we get $c = -k(k^2 + ak + b)$. Therefore, $v_2(c) \geq 2$, contradicting $v_2(c) = 1$.

Now, suppose statement (iv) from Proposition 3.2.2 is holds. Therefore, all iterates $f^n(0)$ are ± 1 or ± 2. Since $f(x)$ is Eisenstein at 2, we get that $f(x) \equiv x \pmod 2$ for every $x \in \mathbb{Z}$, therefore all the iterates $f^n(0)$ are ± 2.

Since $f^n(0) = \pm 2$, we can write $f(x) = x^4 + ax^3 + bx^2 + cx \pm 2$ and the orbit of 0 under $f(x)$ will follow one of the three behaviors in Figures 3.1, 3.2, or 3.3.

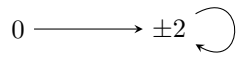

Figure 3.1: Orbit of zero: Option 1

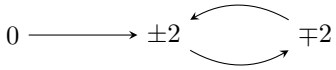

Figure 3.2: Orbit of zero: Option 2

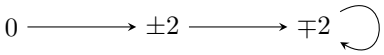

Figure 3.3: Orbit of zero: Option 3

The orbit of 0 can't follow Figure 3.1 since that falls into statement (iii) from Proposition 3.2.2, which we already showed was false.

Suppose the orbit of 0 follows Figure 3.2. Assume $0 \mapsto 2 \mapsto -2 \mapsto 2 \cdots$. Then

$$-2 = f(2) = 16 + 8a + 4b + 2c + 2$$
$$2 = f(-2) = 16 - 8a + 4b - 2c + 2.$$

Subtracting the top equation from the bottom, we get $4 = -16a - 4c$, so $1 = -4a - c$. This contradicts $2 \mid c$. A similar calculation shows that $0 \mapsto -2 \mapsto 2 \mapsto -2 \cdots$ leads to the same contradiction.

Suppose the orbit of 0 follows Figure 3.3. Assume $0 \mapsto 2 \mapsto -2 \mapsto -2 \cdots$. Then

$$-2 = f(2) = 16 + 8a + 4b + 2c + 2$$
$$-2 = f(-2) = 16 - 8a + 4b - 2c + 2.$$

Subtracting bottom equation from the top gives us $16a + 4c = 0$, so $c = -4a$. Since $v_2(a) \geq 1$, we have $v_2(c) \geq 3$, which is a contradiction. A similar calculation shows that $0 \mapsto -2 \mapsto 2 \mapsto 2 \cdots$ leads to the same contradiction. $\square$

CHAPTER 4
SMALL IMAGE

We have been concentrating on the question of when the arboreal Galois representation for f is surjective; that is, when $G_\infty = \mathrm{Aut}(T_\infty)$. Since this is the expected behavior of a generic polynomial, it is also interesting to find provable conditions where $[G_\infty : \mathrm{Aut}(T_\infty)] = \infty$.

Jones gives the following conjecture for quadratic rational maps.

Conjecture 2 (Conjecture 3.11 in [8])**.** *Let K be a global field and $f \in K(x)$ has degree 2. Then $[\mathrm{Aut}(T_\infty) : G_\infty] = \infty$ if and only if one of the following holds:*

(i) The map f is post-critically finite.

(ii) The two critical points γ_1 and γ_2 have a relation of the form $f^{n+1}(\gamma_1) = f^{n+1}(\gamma_2)$ for some $n \geq 1$.

(iii) The root 0 of T_∞ is periodic under f.

(iv) There is a non-trivial Möbius transformation that commutes with f and fixes 0.

The "if"direction for each case is known, but the "only if"direction is open.

In this chapter, we will modify condition (i) and (ii) of Conjecture 2 to a tool that can be used to show $[G_\infty : \mathrm{Aut}(T_\infty)] = \infty$ for degree $d \geq 2$ polynomials.

Recall that the strategy when showing $G_\infty = \mathrm{Aut}(T_\infty)$ is to show H_n is maximal for all $n \geq 1$. The following lemma puts some conditions on H_n that forces G_∞ to have infinite index in $\mathrm{Aut}(T_\infty)$.

Lemma 4.0.1. *Let $f(x) \in K[x]$. Suppose there is an $N \in \mathbb{N}$ such that H_n is not maximal for all $n \geq N$. Then $[\mathrm{Aut}(T_\infty) : G_\infty] = \infty$.*

Proof. Choose $N \in \mathbb{N}$ such that H_n is not maximal for all $n \geq N$. Then

$$\#H_n \leq \frac{(d!)^{d^{n-1}}}{2} \quad \text{for } n \geq N. \tag{4.1}$$

Since $\#G_n = \prod_{k=1}^{n} \#H_k$, we have

$$\#G_n \leq \frac{(d!)^{\sum_{k=1}^{n} d^{k-1}}}{2^{n-N+1}} = \frac{\#\mathrm{Aut}(T_n)}{2^{n-N+1}}. \tag{4.2}$$

So $[\mathrm{Aut}(T_n) : G_n] \to \infty$ as $n \to \infty$, therefore $[\mathrm{Aut}(T_\infty) : G_\infty] = \infty$. □

Let $f(x)$ be a polynomial and let a and b be in $\mathbb{C}$. We will write $a \sim b$ when there is a $k \in \mathbb{N}$ such that

$$f^k(a) = f^k(b).$$

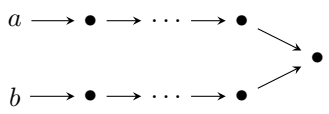

Figure 4.1: $a \sim b$

If L_{n-1}/K_{n-1} is maximal, then $\prod \delta_i \notin K_{n-1}^{*2}$. Let D_n be as in Lemma 2.2.7. In that lemma, we showed $D_n \sim \prod_{i=1}^{d^{n-1}} \delta_i$, where $\sim$ means similar up to squares. So if we can show there is an N where $\prod \delta_i \in K_{n-1}^{*2}$ for all $n \geq N$, then $[\mathrm{Aut}(T_\infty) : G_\infty] = \infty$.

Lemma 4.0.2. *Let $f(x) \in K[x]$ be an odd degree polynomial. Write $d = 2k+1$. Let $\gamma_1, \ldots, \gamma_{2k} \in K$ be the critical points of $f(x)$. Suppose that after relabeling we get*

$$\gamma_1 \sim \gamma_2, \ldots, \gamma_{2k-1} \sim \gamma_{2k}.$$

Then $[\mathrm{Aut}(T_\infty) : G_\infty] = \infty$. See Figure 4.2.

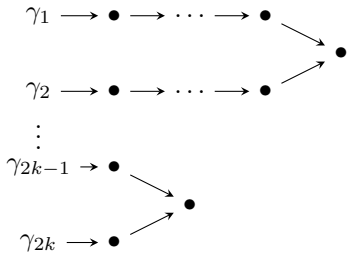

Figure 4.2: Critical point behavior in Lemma 4.0.2.

Proof. Let D_n be as in Lemma 2.2.7, then $D_n \in K_n^{*2}$. There is a $B \in K$ where for $n \geq 2$, $D_n = B \prod_{i=1}^{d-1} f^n(\gamma_i)$. Since $\gamma_1 \sim \gamma_2, \ldots, \gamma_{2k-1} \sim \gamma_{2k}$, there is a N where

$$f^n(\gamma_1) = f^n(\gamma_2), \ldots, f^n(\gamma_{2k-1}) = f^n(\gamma_{2k}) \quad \text{for all } n \geq N.$$

Let $n \geq \max\{N, 2\}$. Put $b_n = \prod_{k \text{ even}} f^n(\gamma_k) \in K$, then $b_n^2 = \prod_{i=1}^{d-1} f^n(\gamma_i)$ and $D_n = Bb_n^2$. Since the critical orbit of f avoids zero, we have $b_n \neq 0$. We have $D_{n+1} \in K_n^{*2}$ since

$$\begin{aligned} D_{n+1} &= Bb_{n+1}^2 \\ &= \frac{b_{n+1}^2}{b_n^2} Bb_n^2 \\ &= \left(\frac{b_{n+1}}{b_n}\right)^2 D_n \in K_n^{*2}. \end{aligned}$$

So L_n/K_n is not maximal for all $n \geq \max\{N, 2\}$, so $[\mathrm{Aut}(T_\infty) : G_\infty] = \infty$. □

Lemma 4.0.3. *Let $f(x) \in K[x]$ be a degree d polynomial. Let $\gamma_1, \ldots, \gamma_{d-1} \in K$ be the critical points of $f(x)$. Suppose that after relabeling the γ_i there is an l such that $2l \leq d-1$,*

$$\gamma_1 \sim \gamma_2, \ldots, \gamma_{2l-1} \sim \gamma_{2l},$$

and γ_k is preperiodic for every $k > 2l$. Then $[\mathrm{Aut}(T_\infty) : G_\infty] = \infty$. See Figure 4.3.

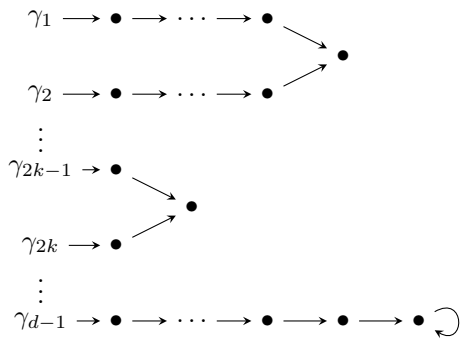

Figure 4.3: Critical point behavior in Lemma 4.0.3

Proof. If $2l = d-1$ then we are done by Lemma 4.0.2, so let's assume that $2l < d-1$. Let D_n be as in Lemma 2.2.7, then $D_n \in K_n^{*2}$. There is a B where $D_n = B\prod_{i=1}^{d-1} f^n(\gamma_i)$ for $n \geq 2$. Notice that $D_n = B\prod_{i=1}^{2l} f^n(\gamma_i) \prod_{i=2l+1}^{d-1} f^n(\gamma_i)$. Since $\gamma_1 \sim \gamma_2, \ldots, \gamma_{2l-1} \sim \gamma_{2l}$, there is a N where

$$f^n(\gamma_1) = f^n(\gamma_2), \ldots, f^n(\gamma_{2l-1}) = f^n(\gamma_{2l})$$

for all $n \geq N$. Let $n \geq \max\{N, 2\}$ and put $b_n = \prod_{\substack{k \text{ even} \\ k \leq 2l}} f^n(\gamma_k) \in K$, then $\prod_{i=1}^{2l} f^n(\gamma_i) = b_n^2$. Notice that $b_n \neq 0$ since the critical orbits avoid zero. Define

$$X = \left\{ \prod_{i=2l+1}^{d-1} f^n(\gamma_i) : n \geq \max\{N, 2\} \right\}.$$

The set X is finite since γ_k is preperiodic for $2l+1 \leq k \leq d-1$. For $x \in X$, define $n_x \geq \max\{N, 2\}$ to be the first n such that $x = \prod_{i=2l+1}^{d-1} f^n(\gamma_i)$. Let $M = \max\left(\{N, 2\} \cup \{n_x : x \in X\}\right)$. Then for $n \geq M$ we have $D_{n+1} \in K_n^{*2}$ since

$$\begin{aligned}
D_{n+1} &= B b_{n+1}^2 x && \text{for some } x \in X \\
&= B b_{n+1}^2 \prod_{i=2l+1}^{d-1} f^{n_x}(\gamma_i) && \max\{N, 2\} \leq n_x \leq M \\
&= \frac{b_{n+1}^2}{b_{n_x}^2} B b_{n_x}^2 \prod_{i=2l+1}^{d-1} f^{n_x}(\gamma_i) \\
&= \left(\frac{b_{n+1}}{b_{n_x}}\right)^2 D_{n_x} \\
&\in K_{n_x}^{*2} && \text{Lemma 2.2.7 } (ii) \\
&\subseteq K_n^{*2}.
\end{aligned}$$

So L_n/K_n is not maximal for all $n \geq M$, so $[\mathrm{Aut}(T_\infty) : G_\infty] = \infty$. □

In the next proposition, we show that the condition that the critical points of $f(x)$ are in K from Lemma 4.0.3 can be dropped.

Proposition 4.0.4. *Let $f(x) \in K[x]$ be a degree d polynomial. Let $\gamma_1, \ldots, \gamma_{d-1}$ be the critical points of $f(x)$. Suppose that after relabeling the γ_i there is an l such that $2l \leq d-1$,*

$$\gamma_1 \sim \gamma_2, \ldots, \gamma_{2l-1} \sim \gamma_{2l},$$

and γ_k is preperiodic for every $k > 2l$. Then $[\mathrm{Aut}(T_\infty) : G_\infty] = \infty$.

Proof. Define $K^C = K(\gamma_1, \ldots, \gamma_{d-1})$ and $K_\infty^C = K_\infty(\gamma_1, \ldots, \gamma_{d-1})$. Also, define $G_\infty^C = \mathrm{Gal}(K_\infty^C / K^C)$, then $G_\infty^C \trianglelefteq G_\infty$. By Lemma 4.0.3, we have $[\mathrm{Aut}(T_\infty) : G_\infty^C] = \infty$. The group G_∞^C is a finite index subgroup of G_∞. See Figure 4.4.

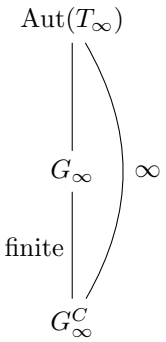

Figure 4.4: Subgroups of Aut(T_∞)

So $[\mathrm{Aut}(T_\infty) : G_\infty] = \infty$. □

BIBLIOGRAPHY

[1] Wayne Aitken, Farshid Hajir, and Christian Maire. Finitely ramified iterated extensions. *International Mathematics Research Notices*, 2005(14):855–880, 2005.

[2] Robert Benedetto, Xander Faber, Benjamin Hutz, Jamie Juul, and Yu Yasufuku. A large arboreal galois representation for a cubic postcritically finite polynomial. arXiv:1612.03358, 2016.

[3] Robert L Benedetto and Jamie Juul. Odoni's conjecture for number fields. *arXiv preprint arXiv:1803.01987*, 2018.

[4] Keith Conrad. Totally ramified primes and eisenstein polynomials, 2009.

[5] David Steven Dummit and Richard M Foote. *Abstract algebra*, volume 3. Wiley Hoboken, 2004.

[6] Paul Garret. Newton polygons. `http://www-users.math.umn.edu/~garrett/m/number_theory/newton_polygon.pdf`, 2005.

[7] Rafe Jones. The density of prime divisors in the arithmetic dynamics of quadratic polynomials. *J. Lond. Math. Soc. (2)*, 78(2):523–544, 2008.

[8] Rafe Jones. Galois representations from pre-image trees: an arboreal survey. In *Actes de la Conférence "Théorie des Nombres et Applications"*, volume 2013 of *Publ. Math. Besançon Algèbre Théorie Nr.*, pages 107–136. Presses Univ. Franche-Comté, Besançon, 2013.

[9] Rafe Jones and Michelle Manes. Galois theory of quadratic rational functions. *Comment. Math. Helv.*, 89(1):173–213, 2014.

[10] Jamie Juul. Iterates of generic polynomials and generic rational functions. arXiv:1612.03358, 2014.

[11] Borys Kadets. Large arboreal galois representations. *arXiv preprint arXiv:1802.09074*, 2018.

[12] Neal Koblitz. *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, volume 58. Springer Science & Business Media, 2012.

[13] Nicole Looper. Dynamical galois groups of trinomials and odoni's conjecture. arXiv:1609.03398, 2016.

[14] R. W. K. Odoni. The Galois theory of iterates and composites of polynomials. *Proc. London Math. Soc. (3)*, 51(3):385–414, 1985.

[15] Brian Rice. Primitive prime divisors in polynomial arithmetic dynamics. *Integers*, 7(1):Paper–A26, 2007.

[16] Joel Specter. Polynomials with surjective arboreal galois representations exist in every degree. *arXiv preprint arXiv:1803.00434*, 2018.

[17] Michael Stoll. Galois groups over $\mathbf{Q}$ of some iterated polynomials. *Arch. Math. (Basel)*, 59(3):239–244, 1992.